Name:	Privacy Policy and Procedures
Endorsed by:	Continuous Improvement and Management Committee
Date approved:	July 2021
Review Date:	January 2023

PURPOSE

Benchmark College is committed to protecting employee and client privacy and confidentiality to the extent permissible by law. However, to achieve the required outcomes of its operations and services, the organisation collects information about its students and their employers (where applicable). Bound by the Australian Privacy Principles, this policy describes how Benchmark College takes reasonable measures to protect the privacy of its staff and students, in line with state and federal legislation.

SCOPE

This document applies to the reasonable measures the organisation takes regarding collection, handling and disclosure of all information that identifies an individual, including both clients and staff of Benchmark College. This policy does not cover internal operations or business practices such as billing, financial auditing or planning.

RELEVANT STANDARDS, GUIDELINES, LEGISLATION & REGULATIONS

- National VET Data Policy – Version 3
- Privacy Act 1988
- Privacy Amendment (Enhancing Privacy Protection) Act 2012
- Office of the Australian Information Commissioner's (OAIC) Australian Privacy Principles Guidelines
- Guide to developing an APP privacy policy
- Australian Skills Quality Authority (ASQA) – Data Provision Requirements
- Student Identifiers Act 2014
- Student Identifiers Amendment (Enhanced Student Permission) Act 2020
- Standards for Registered Training Organisations (RTOs) 2015 – aspects of Standards 1, 2, 3, 5, 6, 7, and 8
- National Vocational Education and Training Regulator Act 2011
- VET Student Loans Act 2016
- VET Student Loans Rules 2016
- Smart and Skilled Contract Terms and Conditions (current)
- Smart and Skilled Operating Guidelines, Notification of Enrolment Process 6 (a)

RELATED DOCUMENTS

- Student Handbook
- Staff Induction Manual
- Consumer Protection Policy
- Records Retention Policy and Procedures
- Complaints and Appeals Policy and Procedures
- Document Control Policy and Procedures
- Enrolment Form
- Application Form
- Student records
- VET Student Loans (VSL)
- AVETMISS data
- Complaints records
- Complaints and Appeals Register
- Incident Management Policy and Procedures
- Critical Incident Form
- Critical Incident Register
- Archive Box Records

DEFINITIONS

APP Entity	An APP (Australian Privacy Principles) Entity is defined to be an agency or organisation[1]
AVETMISS data	The Australian Vocational Education and Training Management Information Statistical Standard (AVETMISS) is a national data standard that ensures consistent and accurate capture and reporting of Vocational Education and Training (VET) information about students. This reporting requirement is part of the Data Provision Requirements that are established by agreement of Training Ministers across Australia under the National Vocational Education and Training Regulator Act 2011[2]
Data Breaches	When personal information held by an agency or organisation is lost or subjected to unauthorised access, use, modification, disclosure, or other misuse[3]
Direct Marketing	Direct marketing involves the use or disclosure of personal information to communicate directly with an individual to promote goods and services[4]
Moderation of Assessments	Moderation is the process of bringing assessment judgements and standards into alignment. It is a process that ensures the same standards are applied to all assessment results within the same Unit(s) of Competency. It is an active process in the sense that adjustments to assessor judgements are made to overcome differences in the difficulty of the tool and/or the severity of judgements[5]
OAIC	The Office of the Australian Information Commissioner (OAIC) is an independent statutory agency within the Attorney General's portfolio[6]
Personal information	*Information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable.* Common examples are an individual's name, signature, address, telephone number, date of birth, medical records, bank account details and commentary or opinion about a person[7]
Police Certificates and Police Checks	A police certificate is a report of a person's criminal history; a police check is the process of checking a person's criminal history. The two terms are often used interchangeably in aged care. Police certificates, not more than three years old, must be held by: ▪ all staff members who are reasonably likely to have access to care recipients, whether supervised or unsupervised; and ▪ volunteers who have unsupervised access to care recipients[8]
Reasonable measures	Benchmark College has put in place reasonable security safeguards and takes reasonable steps to protect the personal information held from loss and from unauthorised access, use, modification or disclosure, or other misuse[9]
Sensitive information	A type of personal information and includes information about: an individual's racial or ethnic origin; health information; political opinions; membership of a political association, professional or trade association or trade union; religious beliefs or affiliations; philosophical beliefs; sexual orientation or practices; criminal record; genetic information; biometric information that is to be used for certain purposes; biometric templates[10]
Tax file numbers	Tax file numbers (TFNs) are unique numbers issued by the Australian Taxation Office (ATO) to identify individuals, corporations and others who lodge income tax returns with the ATO[11]
Unique Student Identifier	USI is a reference number made up of numbers and letters. It creates a secure online record of nationally recognised training that the holder can access anytime and anywhere[12]
Validation of assessment/ program	Involves checking that the program/assessment tool can produce evidence that is valid, reliable, sufficient, current and authentic to enable reasonable judgements to be made as to whether the requirements of the relevant aspects of the Training Package or accredited course had been met. It includes reviewing and making recommendations for future improvements to the assessment tool, process and/or outcomes prior to their use.
VET Student Loans	The VET Student Loans (VSL) program is an Australian Government loan program that helps eligible students enrolled in approved courses at approved course providers pay their tuition fees[13].
Working With Children Check	Working With Children Check is a prerequisite for anyone in child-related work. It involves a national criminal history check and review of findings of workplace misconduct. If individuals are in child-related work they are required to have a Working With Children Check. The Working With Children Check is a prerequisite for paid and unpaid child-related work[14]

[1] The Office of the Australian Information Commissioner (OAIC), Australian Privacy Principles guidelines
[2] http://www.ncver.edu.au viewed on 30 May 2014
[3] http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/data-breach-notification-a-guide-to- handling-personal-information-security-breaches
[4] http://www.oaic.gov.au/images/documents/privacy/applying-privacy-law/app-guidelines/chapter-7-app-guidelines-v1.pdf
[5] http://www.nssc.natese.gov.au/__data/assets/pdf_file/0012/51024/Validation_and_Moderation_-_Implementation_Guide.pdf
[6] http://www.oaic.gov.au/about-us/who-we-are
[7] http://www.oaic.gov.au/privacy/what-is-covered-by-privacy
[8] http://www.health.gov.au/internet/main/publishing.nsf/Content/655FBF4102EF8CADCA257BF0001F9754/$File/police_check_guidelines.pdf
[9] http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-guides/Data_breach_notification_guide_April2012FINAL.pdf
[10] http://www.oaic.gov.au/privacy/what-is-covered-by-privacy
[11] http://www.oaic.gov.au/privacy/privacy-act/tax-file-numbers
[12] https://www.usi.gov.au/about
[13] VET STUDENT LOANS, INFORMATION FOR STUDENTS APPLYING FOR VET STUDENT LOANS - 2017
[14] http://www.kids.nsw.gov.au/Working-with-children/New-Working-with-Children-Check/Who-needs-the-check-/Who-needs-the-Check-

POLICY

Summary Notice

Benchmark College collects personal information to carry out its functions properly and efficiently. Benchmark College only collects personal information that is required for the purposes of employment or education, requests for Australian Government fee assistance or to meet government reporting requirements.

Benchmark College policies and procedures abide by the Australian Privacy Principles and outline reasonable measures taken to protect the privacy of individuals and staff in line with state and federal legislation.

A mechanism exists in which individuals and staff can raise a complaint in relation to how their personal information is handled. All relevant student policies and procedures are available on the Benchmark College website.

The National VET Data Policy states that:

'7.1 It is the responsibility of RTOs to ensure that students who provide an RTO with personal information that will be included in the National VET Provider Collection are reasonably aware that the information may be used or disclosed for the purposes set out in the Privacy Notice at Schedule 1 of the Policy[15]'.

Rights and Choices of Individuals

The rights and choices of individuals and staff

1. Benchmark College has processes and systems in place that protect personal information and individuals are provided with details to access that information;
2. Information collected is only used for the purpose it is intended;
3. Access to view records and/or to correct personal information is available upon request;
4. Ability to make a complaint, if dissatisfied with how private information has been handled, stored or used;
5. Disclosure of information – information is not disclosed to a third party without the individual's written consent;
6. Information available to individuals that ascertains how breaches to this Privacy Policy and Procedure are managed/regulated;
7. Information on how personal information is stored and destroyed.

Information Collected and how it is used

The type of information collected and held by Benchmark College includes: personally identifiable information, including sensitive information, about students (and guardians, where a student is under 18 years of age) before, during and after the completion of training. Consent for student information is gained at application via the application and enrolment forms.

Information may include;

- Student name
- Student date of birth
- Current and previous address details
- Contact information
- Driver's Licence or other identification details
- Relevant Visa (if applicable)
- File notes
- Records of previous training and qualifications

[15] https://www.dese.gov.au/national-vet-data/fact-sheets/national-vet-data-frequently-asked-questions

- Fee payment information, such as bank account details
- Other AVETMISS data (see 'Definitions' section of this document)
- Unique Student Identifier (USI)

Benchmark College also collects personal and professional information from staff to meet its obligations with regards to employment, legal requirements and taxation purposes.

Other/Sensitive Information

Personal information will be collected by Benchmark College due to qualification requirements such as work experience and due to the National Skills Standards Council Determination for Trainers and Assessors. Benchmark College may require the following checks for applicable students/clients/trainers and assessors:

- Working With Children Check
- National Police Check

For more information on the above checks, see the 'Definitions' section of this policy.

Access to sensitive financial information is kept secure by restricting access to approved staff.

How Information is Collected

Generally, information is provided to Benchmark College by the individuals themselves. Individuals provide personal information in person, online, via email and/or by completing various forms, including:

- General course enquiry
- Online enquiry (via the College website)
- Application form
- Enrolment form
- Application for Recognition
- Application for Credit Transfer
- Verification of Qualifications Consent
- Assessment task submission
- Information release form
- Unit Assessment Record
- Working With Children Check (applicable to staff and students)
- National Police Check (applicable staff and students)
- Enrolment data for intended eCaf (Vet Student Loans)
- NSW Apprenticeship/Traineeship Training Plan

In some situations, information could be provided to Benchmark College by a third party. Examples may include other Registered Training Organisations, employers, apprenticeship centres and job seeker agencies.

How we hold information

Depending on the circumstances, we may hold individual's information in either hardcopy or electronic form, or both. Our student/client database is held in electronic format. For more information, refer to *Storage, security and destruction of personal information* section of this Policy.

How information is used

Benchmark College only uses information for its intended purpose. We use personal information:

- For data reporting, such as –
  - the annual AVETMISS data collection
  - Quality indicator reporting (RTOs are required to collect and report their performance against the learner questionnaire, employer questionnaire and competency completion quality indicators to the Australian Skills Quality Authority).
  - Reporting as required by state government training contracts

- For internal purposes such as assessments policies, procedures and processes, risk management, audits (both regulatory and financial), program and assessment validation and moderation and staff training
- To identify, and inform individuals of transitioning of training packages or qualifications in which they may be enrolled in, and
- To administer our customer relationship with individuals.

Unique Student Identifier (USI)

The Unique Student Identifier requirements came in place on 1st January 2015 as a result of the passage of the *Student Identifiers Act 2014*. Students undertaking nationally recognised training delivered by a Registered Training Organisation (RTO) must have a Unique Student Identifier (USI). The USI creates a secure online record of nationally recognised training that the holder can access[16]. The USI is linked to the National Vocational Education and Training (VET) Data Collection.

The Student Identifiers Registrar collects personal information that is reasonably necessary for, or directly related to, its functions and activities pursuant to the *Student Identifiers Act 2014*. The Registrar will only use and disclose personal information for the purposes it was collected for and in accordance with the Privacy Act[17].

In addition to the above, the *Student Identifiers Amendment (Enhanced Student Permissions) Act 2020* came into effect in May 2020 and amended the *Student Identifiers Act 2014*.

The amendments allow a student or person who has studied a VET course after 1st January 2015 to choose whether a licensing body, employment agency or potential employer views their authenticated VET transcript.

The student controls:

- Whether to share their transcript or not
- Who gets access
- Which of their VET achievements are displayed
- How long the transcript can be looked at

The student can remove this access at any time.

The amendments also introduce civil penalties to protect the integrity of the student identifier and authenticated VET transcript and to deter persons from doing the wrong thing.

[16] https://www.usi.gov.au/about
[17] https://www.usi.gov.au/documents/privacy-policy

Disclosure (Sharing)

Information collected or held by Benchmark College will only be disclosed to third parties after written consent has been obtained by the individual concerned, using the Course Enrolment form, or where required by law. Information may be disclosed to the following:

- The individual's authorised representative or legal advisors
- Benchmark College's authorised representative or legal advisors
- Government and Statutory Authorities where required by law
- National VET Regulator auditing purposes
- Job Services Providers

Benchmark College will make all reasonable efforts to secure and protect confidential information from unlawful disclosure. No personally identifiable information will be disclosed by Benchmark College without the consent of the individual(s) concerned.

For the purpose of this document, Benchmark College does not disclose personal information to overseas recipients. An 'overseas recipient' is a person who receives personal information from an APP entity (organisation) and is:

- not in Australia or an external Territory;
- not the APP entity disclosing the personal information; and
- not the individual to whom the personal information relates.

VET Student Loans – Use of Information

Under the *VET Student Loans Act 2016* (VSL Act), each of the following VET officers may use VET information in his or her capacity as a VET officer:

- an officer of a Tertiary Admission Centre
- an officer of an approved course provider
- an officer of a tuition assurance scheme operator that is a party to an approved tuition assurance arrangement
- an officer of an approved external dispute resolution scheme operator.

Further, a VET officer may disclose VET information to another VET officer if the officer believes on reasonable grounds that the disclosure is reasonably necessary for the purposes of the exercise of the powers, or the performance of the functions or duties, in relation to the VSL Act.

Access and requests for information correction

Individuals may request access to the personal information held and may also make requests to correct personal information if it is not accurate, up-to-date or complete. Individuals may request access to their personal information at any time by calling Benchmark College during office hours or sending a written request to Benchmark College by email, facsimile or post (see contact details below). To protect the privacy of our students/clients and the privacy of others, Benchmark College will ask for evidence of identity (refer to procedures) before the College can grant access to information or change it. Once an individual's identity has been verified, access will to be provided in an appropriate manner within thirty (30) business days.

In rare circumstances, and only where it is permitted under the *Privacy Act 1988 (Cth)*, we may not be able to provide individuals with access to information; for example, where it will have an unreasonable impact upon the privacy of others, where it relates to legal proceedings between us through which the information would not otherwise be available, where it would be prejudicial to negotiations, where we are required by law to withhold the information or where it would reveal information relating to our commercially sensitive decision making processes. If we are unable to provide individuals with access, we will provide an explanation in writing within five (5) business days.

Complaints

Individuals may make a grievance or complaint about how their personal information is handled, without incurring a fee (refer to the contact details below for access to these services).

For more information, please refer to the Benchmark College Complaints and Appeals Policy and Procedures found on our website currently available at www.benchmark.edu.au/policies-preocedures

Protecting Personal Information

To help protect the privacy of data and personal information that the College collects and retains, the College uses physical, technical and administrative safeguards. We update and test our security technology on an ongoing basis.

All employees undergo privacy training at regular staff Operations Meetings or Trainer/Assessor meetings that emphasises the importance of confidentiality and the maintenance of student/employer privacy and security of personal information. Access to personal information is restricted to employees who need it to provide benefits or services to students/clients, also refer to '*How information is used'* section of this Policy.

Website

The Privacy Policy and Procedure is published free of charge on our website, currently available at www.benchmark.edu.au The Benchmark College website may contain links to other websites. Please be aware that the College is not responsible for the privacy practices of such other sites. If individuals go to other websites, the College advises caution and to read the related site's privacy policy.

Direct Marketing

Benchmark College practices ethical direct marketing. Where Benchmark College is permitted to use or disclose personal information for direct marketing, it must always: allow an individual to request not to receive direct marketing communications (also known as 'opting out'), and comply with that request. The College will, on request, provide its source for an individual's personal information, unless it is impracticable or unreasonable to do so.

Storage, Security and Destruction of Personal Information

For the purposes of this policy, records include:

- Student Results
- Qualifications / Statements of Attainment
- Completed Assessment Results
- Assessment Tools
- Administrative Records
- Student File
- RTO Management Records (policies & procedures, registers, etc.)

To ensure records are maintained in a safe and suitable condition, the following policy applies:

- Records are kept securely to prevent them being accessed by any non-authorised personnel.
- Records are kept confidential to safeguard information and to protect the privacy of students, employers and Benchmark College staff.
- Through effective hazard reduction identification monitoring procedures, records are kept in such a manner to avoid damage by fire, flood, termites or any other pests.
- Student results and Certificates / Statements of Attainment are backed-up and stored electronically and are available to be retrieved by authorised persons at any time.
- Electronic Certificate/ Statement of Attainment records are kept for thirty (30) years.

- Hard copy records are kept for a minimum of three (3) years from the time the student completes or withdraws from their course.
- Where a complaint/appeal has been registered, the student file is kept for three (3) years. Records of complaints and appeals are kept in the Complaints and Appeals Register for a period of seven (7) years.
- All records relating to VET Student Loans are kept indefinitely.
- Electronic data is backed-up and kept off-site.

Active Records

The Compliance Manager will use Google Drive to regulate, review and edit policies and procedures, courseware, forms and templates. The Chief Executive Officer (CEO) and/or owner(s) of the policy will approve changes to the policies and procedures.

Policies and procedures, courseware, forms and templates are stored in the organisation's shared drive within Google Drive in a folder with restricted access only to relevant staff members. The location of the folder is accessible to relevant staff so that they can access controlled documents.

Documentation records are created, securely managed and disposed of in accordance with the registering body's and legal requirements. Records of business activities are kept in accordance with state and commonwealth requirements. These records include, but are not limited to; Student records, Learning and Assessment records, Governance and Finance records.

Destruction of Records

The CEO is the only person who can authorise the destruction of records. The CEO identifies records for destruction from the Archive Box Records. The CEO provides the approved external storage provider with a work order to destroy identified documents. Records will only be authorised for destruction by the CEO after the retention period has lapsed. To ensure confidentiality, an external approved provider is employed to destroy records.

Electronic Records

All Benchmark College electronic records are controlled using Google Drive or in a folder with restricted access on the shared drive or via a student management system (VETtrak) that can only be accessed by authorised personnel. All policy documents are mapped to Standards for RTO's 2015 and stored in Google Drive.

Google and VETtrak provide their own data protection, security and backup to prevent data loss and unauthenticated access. The IT Manager also performs a Google Drive back up.

The IT Manager will manage the security and access levels to the Google Drive, while the CEO will manage the access and authorisation levels within VETtrak.

Monitoring

The College audits and monitors internal staff on a regular basis to ensure the correct procedures are undertaken for access, handling and destruction of personal information.

Data Breaches

Security is a basic element of information privacy. In Australia, this principle is reflected in the Privacy Act 1988 and the Privacy Amendment (Enhancing Privacy Protection) Act 2012. Benchmark College takes reasonable steps to protect the personal information held from misuse and loss and from unauthorised access, modification or disclosure.

Depending on the circumstances, those reasonable steps may include the implementation of a data breach procedures contained within this policy; notification of the individuals who are or may be affected by a data breach; and notification to the OAIC, may also be a reasonable step.

Appropriate security safeguards for personal information need to be considered across a range of areas. This includes maintaining physical security, computer and network security, communications security and personnel security. To meet information security obligations, Benchmark College undertakes the following activities[18]:

- **Risk assessment** – Identifies security risks to personal information held by the organisation and the consequences of a breach of security.
- **Privacy impact assessments** – Evaluates, in a systemic way, the degree to which proposed or existing information systems align with good privacy practice and legal obligations.
- **Policy development** – Reviews and updates the policy that implements measures, practices and procedures to reduce the identified risks to information security.
- **Staff training** – Trains staff and managers in security and fraud awareness, practices and procedures and codes of conduct.
- **The responsible person or position** – The CEO is the designated position within the organisation to deal with data breaches. This position has responsibility for establishing policy and procedures, training staff, coordinating reviews and audits and investigating and responding to breaches.

Policy and Procedure Review

The Privacy Policy and Procedure is reviewed every 18 months, or in line with legislation or regulation changes. The most recent version of the Privacy Policy and Procedure is uploaded and available on our website, currently available at www.benchmark.edu.au, free of charge. Individuals can request a copy of the document to be printed, posted or emailed to them.

Where policy reviews occur, the College will send all current students an SMS alerting them of the updated policy and where to access it.

Effectiveness of this policy and procedure is monitored by the organisation's Continuous Improvement Committee and Management Committee.

[18] The Office of the Australian Information Commissioner (OAIC), April 2012, *Data breach notification - A guide to handling personal information security breaches*

PROCEDURES

Records Retention

For information regarding records retention, please refer to the Records Retention Policy and Procedures.

Requests for Personal Information

Students may request access to their personal information by calling Benchmark College during office hours or sending a written request to Benchmark College by email, post or in person (see contact details below). To protect the privacy of our students/clients and the privacy of others, Benchmark College will ask for evidence of identity by requesting a minimum of three (3) of the following identifying information:

1. The student's first name and last name (surname);
2. Address, including post code;
3. Date of birth;
4. Phone number;
5. Place of employment (where applicable)
6. Course enrolled in with Benchmark College

The staff member taking the enquiry will confirm this information is correct by accessing the student database system (VETtrak).

Once an individual's identity has been verified, access will be provided in an appropriate manner within thirty (30) business days.

Data Breaches[19]

Step 1: Contain the breach and do a preliminary assessment

- Immediately contain the breach. Stop the unauthorised practice, recover the records, or shut down the system that was breached. If it is not practical to shut down the system, or if it would result in loss of evidence, revoke or change computer access privileges or address weaknesses in physical or electronic security.
- Assess whether steps can be taken to mitigate the harm an individual may suffer as a result of a breach.
- The CEO is made aware of the breach. The CEO determines who else needs to be made aware of the breach (internally and potentially externally) at this preliminary stage.
- Appropriate records of the suspected breach are maintained, including the steps taken to rectify the situation and the decisions made.
- Critical Incident Form is completed and submitted for investigation.

Step 2: Evaluate the risks associated with the breach

To determine what other steps are immediately necessary, the risks associated with the breach are assessed. The following factors are considered when assessing the risk(s):

- the type of personal information involved;
- the context of the affected information and the breach;
- the cause and extent of the breach;
- the risk of serious harm to the affected individuals;
- the risk of other harms.

[19] The Office of the Australian Information Commissioner (OAIC), April 2012, *Data breach notification - A guide to handling personal information security breaches*

Step 3: Notification

The particular circumstances of the breach are considered, and;

- who should be notified and notify affected individuals, and
- what information should be included in the notification, and
- who else (other than the affected individuals) should be notified.

Notification to the OAIC of a data breach occurs where the circumstances indicate that it is appropriate to do so:

- Contact the CEO

Step 4: Prevent future breaches

Once the immediate steps are taken to mitigate the risks associated with the breach, an investigation into the cause is initiated and a comprehensive report written including a prevention plan to ensure the breach does not re-occur. A review of the data breach procedure and this privacy policy and procedure forms part of the investigation process.

Monitoring of outcomes of critical review occurs via through the Continuous Improvement Management Committee.