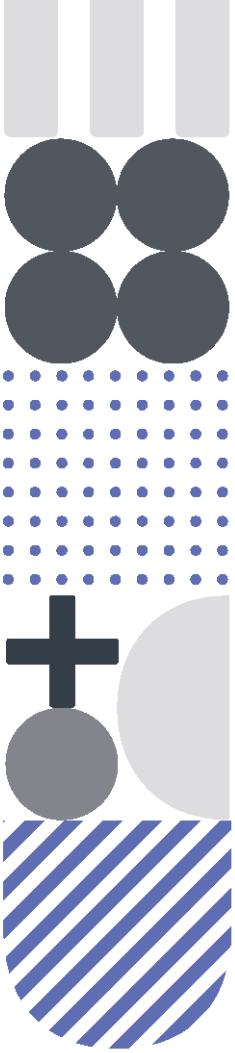
Privacy

POLICY & PROCEDURE



VERSION HISTORY

DATE	VERSION	AUTHOR	APPROVER	REVISION DESCRIPTION
5 Aug 2021	R1	Natalie Darby	Rachelle Matousek	Policy based on version 2.0 from 06 Jan 2020. Updated to new template.
24 Aug 2021	R1.1	Natalie Darby	Rachelle Matousek	Engagement and Monitoring of Partnerships Policy and Procedure changed to: Third Party Arrangements Policy and Procedure.

Privacy

POLICY & PROCEDURE

1 PURPOSE AND SCOPE

In accordance with the Australian Privacy Principles we commit to ensuring all reasonable steps are taken to protect the privacy of our consumers and staff. This policy and procedure outlines how personal information is collected, used, disclosed, stored, destroyed.

This policy and procedure applies to staff, participants, employers, clients and potential consumers and is used throughout all aspects of business operations.

This policy and procedure should be read in conjunction with our 'Consumer Protection Policy and Procedure', 'Record Retention Policy and Procedure' and 'Complaints and Appeals Policy and Procedure'.

1.1 ABBREVIATIONS / DEFINITIONS

AVETMISS	The agreed national data standard for the collection, analysis and reporting of vocational education and training information[1].
Data breach	Where personal information is held by an organisation and is lost or subjected to unauthorised access, use, modification, disclosure or other misuse[2].
NCVER	National Centre for Vocational Education Research Ltd. – the organization responsible for collecting, managing, analysing and communicating research and statistics about the Australian VET sector.
Personal information	Types of information that are specific to an individual for example name, address, contact or bank account details[2].
OAIC	Office of the Australian Information Commissioner
RTO	Registered Training Organisation
Sensitive information	A type of personal information that is sensitive in its nature – for example race or ethnic origin, political opinion, religious belief or affiliation, medical history or criminal record[2].

[1] NCVER (2014) Glossary of VET
[2] Office of the Australian Information Commissioner (2014) Australian Privacy Principles Guidelines

Privacy

POLICY & PROCEDURE

2 GUIDING PRINCIPLES

To operate as an RTO and deliver vocational education, training and assessment we are required to collect a variety of personal information from both consumers and staff members. Where personal and sensitive information is collected it is stored, disclosed and destroyed in accordance with the Australian Privacy Principles (APP). Where we work in partnership with Third Parties to deliver services to consumers we require them to also comply with Australian Privacy Principles.

The following principles underpin this privacy policy and procedure:

- Personal information is protected by the Privacy Act 1988.
- A Privacy Notice, as required by National VET Data Policy 2020 is provided to all participants prior to enrolment.
- We take all reasonable steps required to protect and maintain personal and sensitive information.
- Our procedures are used to assess, plan, implement and review the protection of personal information against misuse, loss, inappropriate access, and inappropriate disclosure.
- Prior to the collection of personal and sensitive information the individual is told what information is to be collected and stored, the purpose of collection, if this information is to be disclosed to a third party and/or under what circumstances disclosure may occur, how third parties will handle individuals' personal information, and how they can contact us regarding their personal information.
- Once the individual is well informed consent is obtained for the collection of information.
- Personal and sensitive information is used only for the purpose of its collection and by staff who require the information to complete their duties.
- Individuals have access to their information when required and without charge.
- Personal information is stored in either an electronic or hardcopy format.
- Security measures such as unique password requirements and restricted file access are used to maintain and protect participant / clients and employee's privacy.
- We will only disclose personal information to a third party where written consent has been obtained from the individual or when compelled by law.
- Where we receive unsolicited information, it is either destroyed or de-identified.
- This 'Privacy Policy and Procedure' is publicly available on our website and a synopsis can be found in the Participant Handbook. More information on the Privacy Act can be found at www.privacy.gov.au

Privacy

POLICY & PROCEDURE

3 PROCEDURE

3.1 TYPES OF INFORMATION COLLECTED AND HELD

Personal and sensitive information is routinely collected from staff and consumers for the purpose of either enrolment or employment.

Information collected for the purpose of enrolment in a qualification or program:

Name	Indigenous status
Address	Proof of identity – 100 Point ID check
Contact details	Unique Student Identifier (USI)
Emergency contact	Disability / special need requirements
Employment history / status	Schooling / qualifications completed
Centrelink information, government allowances	Verification documentation and evidence
Citizenship, Residency and Visa status and information	Vulnerable person checks – National Police Clearance Checks, Working with Children Checks (where specifically requested)
Language, literacy and numeracy assessments	Fee payment information – e.g. credit card information, banking details

Information collected for the purpose of employment:

Name	Recent professional development activities
Address	Reference checks
Contact detail	Insurance documentation
Emergency contact	Proof of identity – 100 Point ID check
Employment history	Superannuation details
Qualifications	Tax File Number
Verification documentation and evidence	Vulnerable person checks – National Police Clearance Checks, Working with Children Checks (where specifically requested)
Registration / Licensing documentation	Bank details

3.2 HOW PERSONAL INFORMATION IS COLLECTED AND STORED

Individuals may disclose information over the telephone, via email, in person and by the completion of relevant forms. Only information disclosed by the individual is used in the collection of information. Prior to the collection of personal information, the individual is told what information is to be collected and stored, the purpose of collection, if this information is to be disclosed to a third party and/or under what circumstances disclosure may occur.

Written and / or verbal consent is obtained prior to collection of personal information and stored appropriately (e.g. in the participant / employee file or on the student management system). For individuals under 18 years of age parent / guardian consent is required.

The types of information collected or disclosed by the individual will vary depending on the method of collection, the purpose of that collection and the individual disclosing the information.

Forms used to collect personal information from participants may include:

- Enquiry forms
- Application forms
- Enrolment forms
- Application for credit transfer form
- Assessment tasks submission forms
- Training plans/ Individualised learning and assessment plans

Documentation used to collect personal information from staff include:

- Application documentation
- Staff details form
- Superannuation documentation
- Competency Record
- Trainer Matrix
- Tax file declaration

Information and assessment evidence collected on the telephone will only be undertaken after consent of the individual is given, information may be kept in the form of a sound recording in electronic format. Such electronic recordings are only retained as long as they are required for the purpose of the individual and are marked for deletion in accordance with our Record Retention Policy and Procedure.

Information is held in either a locked filing cabinet or electronically on our secure cloud-based server. Access to information is limited to personnel with the correct authorisation and is only available to staff for the purpose of collection. Security measures such as unique password requirements and restricted file access are used to maintain and protect participants'/ clients' and employees' privacy. Where staff leave the organisation their access to data is removed / deleted.

Where a prospective student completes an online enquiry or payment – information is held in our email system, secure cloud server or accounting system and is only available to the Finance Manager, Chief Executive Officer or where follow-up is required, finance team for the purpose of reconciliation and issuance of receipt.

3.3 USE OF INFORMATION

Personal information is only for the purpose of its collection and by staff who require the information to complete the tasks associated with their role and function.

Participant personal information is used to:

- Identify individuals enrolled in a program
- Process application and enrolment requests including credit transfer applications
- Process payments for service delivered
- Monitor student progression and provide individualised support
- Enter student assessment results
- Identify participants enrolled in a training product that has been superseded
- Report data required by government (data provision and contractual data requirements)
- Monitor and evaluate organisational performance
- Ensure certification documentation is awarded to the correct graduate
- Serve purposes that are expressly permitted under any agreement with the student

Where participants do not wish to use their name and contact details on assessment task submission sheets, they are able to use their student or enrolment number.

Staff personal information is used to:

- Ensure staff have the correct qualifications, registration / licensing requirements to deliver and assess nationally recognised training.
- To mitigate risk and ensure student safety
- To support human resources processes and systems
- Manage logistical requirements associated with training and assessment
- Meet superannuation and taxation legislative requirements

3.4 DIRECT MARKETING

We only use or disclose personal information for direct marketing purposes if consent has been given by the individual. Individuals can opt to be removed from circulation or subscription lists if they choose not to receive organisation related materials.

3.5 DISCLOSURE OF PERSONAL INFORMATION

We only disclose information to a third party where written consent has been gained from the individual, or when compelled by law. Where possible, data is encrypted so the student has a level of pseudonymity. We do not disclose any individual's personal information to overseas third parties.

We provide all participants with a Privacy Notice via our student management system prior to enrolment, which outlines our legal obligation to disclose participants' personal information to NCVER and how NCVER will handle their information.

We sometimes work in partnership with high quality domestic Registered Training Organisations to deliver Nationally Recognised Training and Assessment and related services, personal information will be disclosed to the relevant RTO (involved in the training course to which the individual is enrolling), for the purpose of that enrolment.

In accordance with legislative and regulatory requirements we, and the other RTO, are required to provide information to State and Commonwealth government departments for the purpose of administration, research and quality assurance[3].

From time to time, we will also disclose personal information (on a confidential basis) to third parties that we use in the ordinary operation of our business, such as account and billing, user experience research and surveys, website hosting and support and maintenance. We will only disclose information to the extent required for the limited purpose of the third party providing services contracted to us so that we may service clients.

We take all reasonable steps to protect the information held from unauthorised access, use and disclosure, however cannot guarantee that our systems and stored data will be completely free from third party interception or are free from corruption.

If consumers have any questions regarding security, they are encouraged to contact us at consumerprotection@momentumconsult.com.au

3.6 ACCESSING AND SEEKING CORRECTION OF PERSONAL INFORMATION

We acknowledge the rights of individuals to have access to their personal information under the 'Freedom of Information Act' and provide opportunities to review this information on request.

Participants and staff are encouraged to update their personal information as it changes to maintain the currency and accuracy of records/data. Where staff identify/suspect that personal information is inaccurate, out of date, incomplete or misleading they will contact the individual for further clarification and action any rectifications as required. Participants are requested to send in writing via email or a letter the updated personal information. Participant records in the student management system are then updated to reflect the new details. There is no charge to an individual who wishes to correct personal information.

[3] AVETMISS data, quality indicator reporting data and information required to undertake a compliance audit.

3.7 DESTRUCTION OF PERSONAL INFORMATION

Personal information disclosed to us will be stored in our student management system for the period required by law. Where a partner or third party RTO is also used, participants should refer to the privacy policy of the relevant third party for more information.

When we no longer require personal information (e.g. completion, withdrawal or cancellation of a student's enrolment), it is destroyed after the required retention period has elapsed. Hard copy information is shredded securely and electronic information is securely deleted.

3.8 COMPLAINTS AND APPEALS

Feedback with regards to compliance with the Privacy Policy is encouraged by contacting the Consumer Protection Officer or by making a complaint.

Consumer Protection
mailto: Consumerprotection@momentumconsult.com.au
T: 1300 564 608

See our 'Complaints and Appeals Policy and Procedure' for more information.

3.9 GOVERNANCE MECHANISMS

We have a robust governance framework in place to ensure our compliance with the Australian Privacy Principles. The following governance framework underpins and supports the operationalisation of this policy and procedure:

- Risk assessments including privacy impact assessments are undertaken when required.
- Staff receive training on the handling of personal and sensitive information on employment commencement and as changes and/ or amendments occur.
- Staff who regularly handle personal information are provided with supervision and support from their line manager.
- Performance development and management processes ensure staff have the knowledge and skills required to complete their role requirements
- Where an agent or contractor is collecting personal information from a consumer on our behalf systematic processes are implemented to monitor compliance and maintain the student's privacy– see *Third Party Arrangements Policy and Procedure*.
- The Privacy Policy and Procedure is publicly available on the website and is summarised in the Participant Handbook.
- This Privacy Policy and Procedure is reviewed and updated annually or where required. Where changes to the Privacy Policy and Procedure have occurred the latest document version will be placed on the website and all participants/clients will be notified by email that a new privacy policy and procedure has been released.
- We take all reasonable steps required to protect and maintain personal and sensitive information in accordance with the Australian Privacy Principles. If a data breach was to occur the organisation has a systematic approach to managing the

critical incident in an open and transparent manner that manages risk effectively. The process for managing a data breach includes:

- conducting a preliminary assessment and investigation
- undertaking a risk assessment
- notifying all relevant parties, and
- developing an action plan to prevent potential future breaches.

- Our management monitors the effectiveness of the policy/procedure and is actively involved in its review.

3.10 REFERENCES

- Australian Skills Quality Authority (2015) "Standards for Registered Training Organisations (RTOs) 2015".
- Education Services for Overseas Students Act 2000
- Privacy Act 1988
- Privacy Amendment Act 2012
- Office of the Australian Information Commissioner () Australian Privacy Principles
- Office of the Australian Information Commissioner (2014) Guide to developing an APP privacy policy
- Department of Education, Skills and Employment (2020) "National VET Data Policy"