

Privacy Policy

1. PURPOSE

The RTO is committed to protecting the privacy and confidentiality of personal information and compliance with all relevant privacy legislation, including current Australian Privacy Principles (APPs). This policy sets out the way we handle personal information in an open and transparent manner, including the use and disclosure of personal information, as well as client rights to access their personal information.

2. SCOPE

This policy applies to all personal information collected or created by The RTO to perform its business (whether on premises or hosted externally on behalf of The RTO, in electronic or physical form). Information and data collected and stored by other parties such as the National VET Regulator, USI Registrar, WHS Regulator, employers, industry bodies and government agencies is subject to legislation and their own internal policies and procedures.

Each RTO staff member is responsible for reading, understanding and putting into practice the Privacy Policy requirements and ensuring The RTO operations comply with its requirements. Potential personal information breaches, concerns or queries need to be raised immediately with the CEO.

3. DEFINITIONS

Eligible or notifiable data breach is defined in the Privacy Act as the 'unauthorised access or disclosure of personal information, or loss of personal information in circumstances where this is likely to occur, that is likely to result in serious harm to any of the individuals to whom the information relates'. Examples include but are not limited to when:

- a device containing personal information is lost or stolen
- hard copy documents containing personal information are lost or stolen
- The RTO database containing personal information is hacked
- The RTO mistakenly provides personal information to the wrong person
- A customer notifies The RTO that their personal information has been accessed or disclosed in an unauthorised way.

Organisations captured by the Privacy Act include 'all businesses and non-government organisations with an annual turnover of more than \$3 million, all health service providers and some small businesses, for example, a contractor that provides services under a Commonwealth contract'.

Personal information under the Privacy Act is 'information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- whether the information or opinion is true or not; and
- whether the information or opinion is recorded in a material form or not.'

Some examples relevant to The RTO include address, employment and other enrolment details, assessment outcomes and third-party reports. It can include verbal, written or electronic data as well as photographs, video or audio recordings.

Sensitive information includes information or an opinion about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, sexual orientation, criminal record, health information and some aspects of genetic and biometric information. Some examples relevant to The RTO include government identifiers such as drivers licence, USI, Medicare card, passport, other forms of identification that could be used for identity fraud, financial information

Serious harm is not defined in the Privacy Act, however, in the context of a data breach, serious harm to an individual may include serious physical, psychological, emotional, financial, or reputational harm.

4. REFERENCES

- Commonwealth Privacy Act (includes APPs + Notifiable Data Breaches)
- Notifiable Breaches Fact Sheets
- NSW Privacy & Personal Information Protection Act
- ASQA Data Collection & Provision Requirements
- ASQA Privacy Policy
- Student Identifiers Act & Regulation
- National VET Data Policy
- AVETMISS VET Provider Collection Specifications.

5. PRIVACY POLICY

5.1 Personal Information collected by the RTO

It is a requirement of government and funding bodies that the RTO collect personal information about a client enrolling in a course/qualification. This information must be reported to the VET Regulator and must comply with relevant legislation and requirements (refer References) above. Information collected includes but is not limited to:

- Name
- Address – residential & postal
- Contact details (telephone & email)
- Date of Birth
- Gender
- Country of birth
- Citizenship
- Whether Aboriginal or Torres Strait Islander
- Language spoken at home
- Disability information
- Education details
- Previous qualifications
- Employment status & employer details
- Reason/s for undertaking study
- LLN or other needs
- Capacity to meet assessment requirements.

The RTO only collects personal information to enable the RTO to fulfil its functions, by fair and lawful means. We will do this in a reasonable and unintrusive manner and will comply with all current Commonwealth & NSW privacy legislation and AVETMISS. We do not collect sensitive information unless in accordance with the APPs as currently in force.

The Enrolment Form & Attendance Form completed by clients contains information outlining why personal information is collected and how it is used. Clients are required to sign that they agree to the use of their personal information as stated and provide authority for the RTO to validate their USI. The RTO enrolment form uses the declaration as set out in the National VET Provider Collection Data Requirements Policy.

Where a person objects to providing background information as requested on the Enrolment Form we may be able to accommodate their objection, but the RTO must still obtain sufficient details to enable accurate identification of the person including obtaining and verifying their USI. Issuance of certification cannot occur without this unless the student has been granted an exemption by the USI Registrar.

5.2 Sources of Personal Information Collected

The RTO only collects personal information directly from each client at enrolment or as the course progresses and only to enable the RTO to fulfil its functions. The RTO does not collect personal information from other sources, except as requested by the client or where permission from the client is provided, for example, to verify authenticity of qualifications or to discuss training issues, reasonable adjustment or outcomes with the employer. Unsolicited information will be assessed within 14 days to determine if it complies with APPs and if not, will be destroyed.

5.3 Advice provided to clients

At the time The RTO collects personal information we will take reasonable steps through our website, Participant Handbook, enrolment form and course induction, to ensure that clients are made aware of:

- The RTO identity and how to contact us
- The client's rights about accessing their personal information
- the purpose for which the personal information was collected
- to whom we disclose personal information
- any law that requires us to collect personal information
- the consequences, if they do not provide the information we require.

5.4 Use and Disclosure

The RTO ensures that the information we receive remains private and confidential. It is used only for the purposes for which the client agrees. Where discussions are required with the employer who has paid for the training, permission to release information is provided upon enrolment. Separate permission may be sought to release information to other stakeholders via email or by completing an Authority to View Documents/Release Information.

The RTO will not reveal, disclose, sell, distribute, rent, license, share or pass personal information on to a third party, other than those that we have a binding agreement with ensuring that the third party affords the personal information similar levels of protection as we do. To provide clients with training and assessment services, we may be required to disclose personal information to third parties such as:

- VET or WHS Regulators
- Commonwealth/State/Territory funding agencies
- National Centre for Vocational Education Research
- Employer.

The release of certain information is mandatory for the purposes of AVETMISS reporting and claiming public funds for the delivery of training and assessment services under Commonwealth/State/Territory government contracts.

Permission for this to occur is provided upon enrolment. Further, The RTO may use and disclose personal information to provide training and assessment services to the client at the point of collection or for another purpose if:

- The client would reasonably expect us to disclose it for that purpose
- That purpose is related to the purpose specified to the client at the time of collection
- The RTO reasonably believes that use or disclosure is necessary to lessen or prevent a serious and imminent threat to an individual's life or health
- The RTO has reason to suspect that unlawful activity has been, or is being engaged in, and the information may be relevant to investigation, or reporting to the relevant authority
- The use and disclosure are specifically authorised or required by law
- The use and disclosure are reasonably necessary for the enforcement of criminal law, law imposing a pecuniary penalty, or for the protection of the public revenue.

The RTO does not use or disclose personal information for the purpose of direct marketing of products or services unless consent is provided. Clients may withdraw consent at any time. Where personal information is used or disclosed a written record is maintained. The RTO does not release information to overseas recipients for any purpose.

5.5 Data Quality & Integrity

The RTO will take all reasonable steps to ensure that personal information is accurate, complete and up-to-date. Clients are encouraged to help us keep their personal information accurate, complete and up-to-date by informing us of any changes to details.

5.6 Data Security & Retention

The RTO is committed to protecting personal information from misuse, loss and from unauthorised access, modification or disclosure. We ensure this by having security measures including:

- Individual password access to internal systems and databases
- Secure file cabinets and compactus (locked and designated personnel access only)
- Electronic data back-up overnight and monthly & stored off-site.

Data is retained in both hard copy and electronic format. We will take reasonable steps to destroy or permanently de-identify personal information if it is no longer required for any purpose.

5.7 Access and Correction

Clients are provided with access to personal information at any time by email request and may request corrections to that information at any time. There is no charge for access or changes to information and all requests will be dealt with within 14 days of receipt. Where changes are made this will be confirmed with the client and any relevant third party will be advised. Where changes are deemed unnecessary the client will be advised in writing of the reasons for the decision and has the option to lodge a complaint using our complaints procedure.

We may refuse access to personal information as outlined in the APPs, including but not limited to, that it may pose a serious threat to an individual or public safety, it is unlawful or relates to information that may be subject to legal proceedings.

5.8 Government Related Identifiers

The RTO will not adopt as its own identifier an identifier that has been assigned by a government agency. Our student database allocates its own student identifier as required by AVETMISS and we also collect and validate the Unique Student Identifier (USI) as required by legislation.

The RTO will not use or disclose any government identifiers except as permitted for the purposes of The RTO, to fulfil legislation obligations or as permitted. Individuals may choose not to identify themselves or may use a pseudonym however this will not apply if legal names are required or it is impractical for The RTO to deal with an issue without actual names. The RTO will provide information to clients if they require an exemption from the USI Registrar.

5.9 Resolving Privacy Concerns

Clients can raise concerns regarding personal information handling practices by contacting The RTO Compliance Manager or CEO by telephone, email or by completing our Complaints Reporting & Action Form. The CEO is responsible for dealing with privacy inquiries, concerns or complaints.

5.10 Use of the Internet/E-Data Storage & Transmission

The RTO takes all reasonable steps to protect personal information security when using e-data storage and transfers. Security of data transmitted to Commonwealth, state and territory bodies is managed by these bodies using Commonwealth government myID system.

5.11 Notifiable Data Breaches (NDB) & Response Plan

All staff comply with privacy legislation including notifiable data breaches and take all necessary steps to always retain any student records under their control in a secure manner.

On course completion at external training sites, RTO records including enrolment forms, student identification, assessments etc. are kept secure until returned to Head Office as soon as reasonably practicable. In addition, student files or other records may only be removed from the RTO premises with the permission of the CEO.

Any requests for information about students must be referred to the RTO Compliance Manager and/or the CEO for review and action.

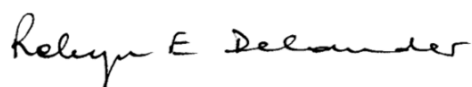
If at any time staff believe personal data may have been inappropriately accessed, disclosed, released, used, interfered with or modified or lost or in some other way the general privacy provisions or notifiable data breach provisions have been breached, they must advise the Compliance Manager and/or CEO immediately so that a response plan can be initiated.

5.12 Data breach response plan

If a breach is identified The RTO will:

- Contain the data breach to prevent any further compromise of personal information
- Assess the data breach and act to remediate any risk of harm
- Notify involved individuals and Regulator if it is an eligible data breach under the NDB scheme, notification is mandatory.
- Review the incident and consider what actions can be taken to prevent future breaches.

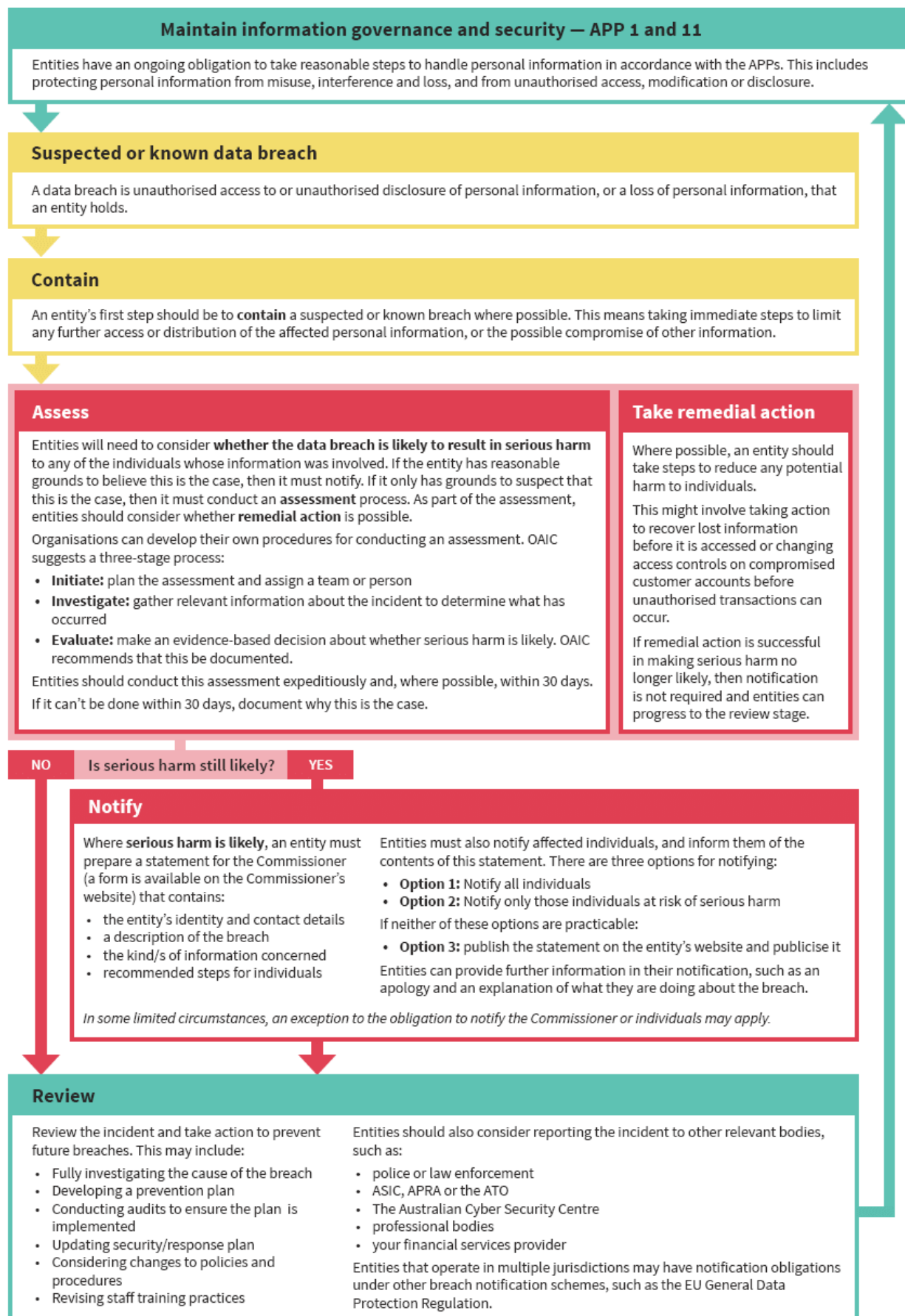
Actions will be taken on a case-by-case basis according to risk. If required to be notified, The RTO will complete the Office of the Australian Information Commissioner's online Notifiable Data Breach form <https://www.oaic.gov.au>



ROBYN DELANDER (CEO)

12 June, 2025

Review Date: 12 June, 2027



Extract from OAIC - Data breach preparation & response guide