# PP4.10 – Privacy Protection

| | |
|---|---|
| Policy area | Governance |
| Standards | Compliance Standards for RTOs, Requirement 20 |
| Responsibility | CEO, General Manager |
| Classification | |

## 1. Purpose

The purpose of this policy is to:

- provide Down to Earth Training and Assessing with a policy framework that enables our compliance with the Privacy Act 1988 (Privacy Act) Australian Privacy Principles (APPs).
- define the approach and circumstances for the collection, use and disclosure of personal information.
- provide strategies to be applied to keep information secure including hard copy and digital information.
- provide a system to classify information that enables the access to, distribution and handling of this information to be controlled.

## 2. Definitions

- **Personal information** means information or opinions that can identify or reasonably identify an individual. This includes an individual's name, signature, address, phone number, date of birth, employee record information, photographs, internet protocol (IP) addresses, biometric data like voice prints and facial recognition (as they capture unique characteristics of a person), and location data from mobile devices, which can disclose patterns or habits of user activity. It is important to note that personal information also includes sensitive information and credit information (see below).

- Although not specifically defined within the Privacy Act personal information should also be taken to include information that is used to verify the identity of a person when collected to establish their eligibility for a training subsidy or to assist them to create a unique student identifier. This can include what is often referred to as "high risk personal information" which includes information such as drivers licence details, passport details, birth certificate, rates notice, Medicare Card details, Visa details, etc. When combined with other personal information

which may be publicly available on social media or through the internet, access to high risk personal information carries heightened risks including the risk of identity theft.

- **Sensitive information** means personal information or opinions concerning an individual's racial or ethnic origin, political opinions, political association memberships, religious beliefs or affiliations, philosophical beliefs, memberships of professional or trade associations, trade union memberships, sexual preferences or practices, criminal records, health information, genetic information that does not constitute health information, biometric information intended for automated biometric verification or identification, and biometric templates.

- **Credit information** means specific details collected and used to evaluate an individual's creditworthiness. This includes the full name, date of birth, sex, current or last known address, previous two addresses, current or last known employer's name, driver's licence number, and information about credit providers that have extended consumer credit to a person, including whether they're licensed by ASIC. It also includes details about the type and terms of consumer credit provided, dates of credit availability and termination, credit limits, repayment obligations, repayment history (including timely or missed payments and financial hardship records), and information regarding credit enquiries made by providers in response to a person's credit applications. Credit information further encompasses records of defaults on payments of $150 or more, statements acknowledging payments previously in default, variations or new credit arrangements resulting from defaults, court judgments related to a person's credit, information recorded on the National Personal Insolvency Index (including bankruptcy and debt agreements), publicly available details regarding a person's creditworthiness, and opinions by credit providers about serious credit infringements a person may have committed.

## 3. Policy statement

Down to Earth Training and Assessing collects and stores personal and sensitive information on our students and industry clients. In doing this, Down to Earth Training and Assessing has introduced this policy to comply with our obligations under the Privacy Act. Protecting personal and sensitive information is essential not only to comply with the Privacy Act but also to safeguard Down to Earth Training and Assessing staff and students from potential financial or reputational harm. Mishandling personal and sensitive data can lead to breaches of trust, significant reputational damage, and potential loss of enrolments, business partners, and revenue. Additionally, losing or compromising personal and sensitive information that is crucial to our operations can severely impact our ability to deliver services effectively.

Implementing robust personal and sensitive information security practices offers tangible benefits, including streamlined and efficient processes within the Down to Earth Training and Assessing

operation. It substantially reduces the risk of privacy breaches and minimises the resources required to manage and resolve any incidents that may occur. Many of the strategies outlined in this policy will also enhance our ability to handle other sensitive information, such as confidential information, effectively and responsibly.

### 3.1 Authority to collect and store information

Down to Earth Training and Assessing is an approved Registered Training Organisation by the National VET Regulator. This registration is issued under the authority of the National Vocational Education and Training Regulator Act 2011. This legislation requires Down to Earth Training and Assessing to collect personal and sensitive information from our students. This requirement is specified in the *Data Provision Requirements 2020* which is one of the legislative instruments that Down to Earth Training and Assessing must comply with as a condition of its registration.

The *Data Provision Requirements 2020* require Down to Earth Training and Assessing to collect data from students in accordance with the Australian Vocational Education Training Information Statistical Standard (AVETMISS). This is a complex information standard that defines information about who the student is, where the training is delivered and what they are studying. The Compliance Standards for RTOs require Down to Earth Training and Assessing to retain and store this information for **up to 30 years** and to report training activity to government agencies in accordance with mandatory reporting requirements.

In addition to the *Data Provision Requirements 2020*, the *Student Identifiers Act 2014* also requires Down to Earth Training and Assessing to collect high risk personal information for the purpose of creating or verifying a student's Unique Student Identifier. Together, these requirements form a statutory obligation to collect, store and report information of any student participating in nationally recognised training with Down to Earth Training and Assessing.

### 3.2 Use of personal information

To comply with its obligations under the *Data Provision Requirements 2020*, the *Student Identifiers Act 2014*, or contractual obligations or to facilitate an outcome of a service offered to students, Down to Earth Training and Assessing will use personal information to comply with reporting obligations to Government agencies at the Commonwealth level and if accessing Government subsidised training also with a relevant State or Territory Government agency. Under some circumstances such as to facilitate an outcome of a service (such as licencing), Down to Earth Training and Assessing may also need to report personal information to other relevant Government or responsible agencies. Students enrolling into a course with Down to Earth Training and Assessing are advised of our collection and use of personal information with the *Student Handbook* sections related to "*Your Privacy*" and "*National VET Data Policy*".

### 3.3 Solicited information

Contact information such as name, organisation, position, address, telephone, and email are collected for marketing, support services, mandatory reporting and for communicating with stakeholders as part of our day-to-day operation.

In addition to the collection of training activity information, Down to Earth Training and Assessing will also collect, store and report information relating to satisfaction surveys, complaint handling and on our client employers.

Names, addresses, phone numbers, emergency contact details, bank account details and other employment related information is collected from employees for the purpose of managing human resources. The management of staff personal information complies with this policy.

### 3.4 Sensitive information

Personal information collected by Down to Earth Training and Assessing that may be regarded as 'sensitive' under the Privacy Act includes:

- 'Disability' and 'long-term impairment status' (health); and 'indigenous status', 'language spoken at home', 'proficiency in spoken English', 'country of birth' (implies ethnic/racial origin). This information is specified in the AVETMISS data elements and is collected for the national VET data collections, national VET surveys, and may be collected for VET-related research.
- 'Dietary requirements' (health-related) are collected for event catering purposes only.
- Biographical information, which may contain information on 'affiliations' and 'membership of a professional or trade association' are obtained from keynote speakers for event marketing purposes.
- 'Memberships of professional associations' and 'health and work injury information' is collected from Down to Earth Training and Assessing employees for HR management purposes.

### 3.5 Direct marketing

Down to Earth Training and Assessing respects an individual's right not to receive marketing material and provides an option within communications and on its website for individuals to unsubscribe from receiving marketing material. Down to Earth Training and Assessing conducts its marketing communications and dissemination of service information in accordance with Australian Privacy Principle 7 (Direct marketing), the Spam Act 2003 (in respect of electronic communications), and the Do Not Call Register Act 2006. It is not Down to Earth Training and Assessing practice to 'cold call' for the purpose of marketing its products and services. Down to Earth Training and Assessing is not to undertake in unsolicited marketing practices, ever.

### 3.6 Unsolicited personal information

Unsolicited personal information is information Down to Earth Training and Assessing may receive without actively asking for it. If Down to Earth Training and Assessing should receive unsolicited personal information, it will be treated and managed according to the APPs. This means Down to Earth Training and Assessing will need to assess the information to determine if holding the information is lawful. This includes assessing if the information could have been collected if actively sought by Down to Earth Training and Assessing in the first place in accordance with Australian Privacy Principle 3 (Collection of Solicited Personal Information) and, is it necessary for Down to Earth Training and Assessing to hold the information to perform its function and service to students? If the answer to either of these questions is no, Down to Earth Training and Assessing is to destroy or de-identify the information as soon as practicable and inform the owner of the information of the actions.

The following is a practical example of protecting unsolicited personal information: A parent of a student sends an email to Down to Earth Training and Assessing with records of their young adult son's medical history and condition. Down to Earth Training and Assessing did not request this information and does not require it for any reasonable purpose in providing services to the student. In this scenario, the General Manager with the CEO should promptly evaluate the information. This evaluation would determine that Down to Earth Training and Assessing could not have lawfully collected private medical information, it must securely destroy or de-identify the information as soon as possible and advise the parent and student of this action.

### 3.7 Notification of collection

Down to Earth Training and Assessing aims to notify individuals of the collection of their personal information before, or at the time of collection, or as quickly as possible thereafter. Notifications are usually in writing but may be verbal by phone. Examples of notification include:

- Marketing – notification is provided on our website course application page. Individuals are also notified at the time of collecting personal information for events. A privacy notice is provided in all Down to Earth Training and Assessing marketing communications.

- Pre-enrolment information supplied to the prospective student prior to their enrolment or commencement includes the Student Handbook. Students enrolling into a course with Down to Earth Training and Assessing are advised of our collection and use of personal information with the *Student Handbook* sections related to "*Your Privacy*" and "*National VET Data Policy*".

- Quality Indicator surveys – notification is provided in the email of invitation to participate in the surveys and also at the time of collecting the information.

- Down to Earth Training and Assessing staff – Notification is provided on employment commencement.

### 3.8 Disclosure of personal information

Down to Earth Training and Assessing is not to disclose personal information other than for the purpose for which it was collected, or an individual has consented to a secondary purpose, or an individual would reasonably expect this (such as receiving communications about upcoming events), or if required by law.

Down to Earth Training and Assessing may share personal information with the Commonwealth government in accordance with Commonwealth contractual or regulatory obligations. In these circumstances, Down to Earth Training and Assessing will take reasonable steps to inform and seek consent from the individuals concerned and take all reasonable steps to ensure that the recipient handles the personal information according to the APPs.

Down to Earth Training and Assessing is not to sell or distribute mailing lists or student contact information to third parties under any circumstance. Down to Earth Training and Assessing does not disclose personal information to overseas recipients. While people around the world can access material published on our website, no publications on our website are to contain identifiable personal information.

### 3.9 Management of personal information

Down to Earth Training and Assessing will ensure the personal information it collects and uses or discloses is accurate, up to date, complete and relevant. Down to Earth Training and Assessing routinely updates the information held in its student management system. This includes confirming with students who are returning for a new enrolment if their personal contact details have changed.

### 3.10 Access to and correction of personal information

Individuals may, subject to the exceptions prescribed by the APPs, request access to and correction of their personal information where this is collected directly from individuals by Down to Earth Training and Assessing.

Down to Earth Training and Assessing does not charge for giving access to or for correcting personal information unless the student is requesting copies to be mad of information which may incur an administrative fee (Refer to *PP1.14 – Student Record Retention and Management*). Requests for access to or correction of personal information should be made in accordance with the access to records arrangements outlined in the *student Handbook* and *PP1.14 - Student Record Retention and Management*.

### 3.11 Retention and recording of high risk personal information

In accordance with the *APPs principles 11.2* and *Student Identifiers Act 2014*, section 11, Down to Earth Training and Assessing is not to continue to hold information where it has no further purpose for this information. An example of this may include high risk personal information (refer to definitions) which may include a copy of a student passport, drivers' licence or Medicare Card. Once the student's identification or eligibility has been verified (the purpose), Down to Earth Training and Assessing is to destroy through shredding or permanently deleting these records so that these records are no longer being stored by Down to Earth Training and Assessing. Down to Earth Training and Assessing's information security risk is significantly reduced if these records are destroyed as soon as possible after the purpose for collecting this information has been satisfied.

Where possible, staff should seek to confirm verification using high risk personal information directly with the student either in person or over video conference and avoid the need to collect and store these records altogether.

Down to Earth Training and Assessing is to retain the details of high risk personal information that is used for the purpose of verification by recording the type of information that was viewed, the date it was viewed and by who. This is an acceptable record for the purpose of meeting our compliance obligations and is an affective risk avoidance strategy that is to be applied. As an example, instead of collecting and storing the actual record the following is acceptable:

*Student Bloggs, NSW Drivers Licence, verified 23 Sep 2025 by Staff Member Bloggs.*

### 3.12 Information security

Down to Earth Training and Assessing is to apply strict security controls over information that it has collected and stores. This includes hard copy and digital records. The following guidelines are provided for the handling and storage of both hard copy and digital records:

i. **Hard copy information security**. All Down to Earth Training and Assessing hard copy information are to be stored to prevent access to unauthorised access. This includes unauthorised access by staff members who have no purpose to access the information to perform their duties. Where possible, the storage of hard copy information is to be minimised with a preference to digitise records that need to be retained. The following strategies are to be applied to the storage and handling of hard copy information:

   a) **Secure storage**. Sensitive information must always be stored securely in locked cabinets or rooms accessible only to authorised personnel.

b) **Controlled access**. Distribution of keys or access codes for locked areas must be limited exclusively to authorised staff, with clear records maintained of all keyholders.

c) **File organisation and labelling**. All information and files are to be clearly labelled and organised consistently to facilitate effective storage and retrieval, while ensuring security and confidentiality. Please refer to information classification guidelines at section 3.13.

d) **Secure disposal**. Outdated or unnecessary sensitive information must be disposed of securely, utilising methods such as shredding to prevent unauthorised access.

e) **Staff training**. New and existing staff are to be trained on proper handling, storage, labelling and confidentiality procedures related to hard copy information.

f) **Office security measures**. Office doors, particularly those leading to areas housing sensitive information, must remain locked whenever unattended or outside of working hours.

g) **Visitor management**. Visitors must be escorted at all times when accessing areas where sensitive records are stored, ensuring continuous monitoring of sensitive document access.

h) **Regular access audits**. Monthly audits are be conducted to verify and update authorisation records for keys and access codes, ensuring access remains restricted and up-to-date.

i) **Digitisation and backup**. Important or critical information should be digitised as appropriate, with electronic copies securely stored and backed up regularly to provide additional protection against loss or damage.

j) **Clean desk policy**. Staff must adhere to a clean desk policy, ensuring all sensitive files and information are secured appropriately at the end of each working day.

ii. **Digital information security.** The following strategies are to be applied to the storage and handling of digital information:

a) **Cybersecurity responsibilities**. The CEO with the support of the General Manager is responsible to oversee information security awareness and compliance.

b) **User access management**. User access to systems and cloud services must be strictly controlled. All users are required to use unique credentials, maintain strong

passwords, update these regularly, and enable multi-factor authentication (MFA) wherever it is available.

c) **Cloud service security**. Down to Earth Training and Assessing authorises the use of trusted cloud-based providers, such as Microsoft 365, Dropbox, Google Drive, or similar services. Permissions for accessing stored data are to be set according to roles and regularly reviewed to ensure appropriate data access.

d) **Device security**. All devices such as computers, printers, routers, etc must have automatic device driver and security updates enabled and regularly maintained. Reliable antivirus software (such as Norton's) must be installed, configured for daily scanning, and kept current, along with active firewall settings to prevent unauthorised network access.

e) **Data encryption and backup**. Sensitive information stored or transmitted by Down to Earth Training and Assessing must be encrypted to ensure privacy and confidentiality. This includes data stored within student management systems. Down to Earth Training and Assessing must verify with third party suppliers of student and learning management systems that the Down to Earth Training and Assessing data stored in these systems is protected by encryption both while in transit and when static. Data backups must be performed regularly and securely stored in cloud services or off-site locations. Down to Earth Training and Assessing must verify the ability of third party suppliers of student and learning management systems to recover and restore services to a restore point that must not exceed 24 hours.

f) **Remote work security**. Personnel must follow clearly defined guidelines for securely working remotely. This includes secure use of collaboration and communication platforms such as Teams or Zoom and avoiding public Wi-Fi networks unless securely connected via VPN.

g) **Staff cybersecurity training**. All staff are to undertake annual privacy and information security training to maintain their understanding of cybersecurity threats and best practices, including recognising phishing attempts, safe password management, and appropriate handling of sensitive information.

h) **Email security**. Down to Earth Training and Assessing email systems is to include active spam filtering, phishing protection, and multi-factor authentication. Staff must use official organisational email accounts for all work communications, and exercise caution with email attachments and links. All email correspondence sent or received using official organisational email accounts remains the property of Down to Earth Training and Assessing.

i) **Website security**. Down to Earth Training and Assessing's website will maintain secure hosting with active SSL certification. The website and all plugins, themes, and extensions must be updated regularly. Security plugins or firewall tools (such as Wordfence) must be implemented to detect, prevent, and alert administrators to potential threats and block unwanted traffic.

j) **Website access controls**. Website administrative access for Down to Earth Training and Assessing must be limited strictly to authorised personnel, who must use secure passwords and MFA. Regular website backups must be securely maintained, and unnecessary files or outdated user accounts routinely removed to mitigate risks.

### 3.13 Information classification labels

Down to Earth Training and Assessing is to use information classification labels to clearly identifying the sensitivity and importance of information being handled by staff, students and partners. Information classification labels guide staff on how to appropriately handle, store, and share information, thereby reducing risks associated with unauthorised disclosure, misuse, or loss of information. Labels support compliance with legal and regulatory obligations, helping Down to Earth Training and Assessing avoid potential penalties and safeguard our reputation. Additionally, clear labelling of information promotes consistent information security practices across our operation, reinforcing staff accountability and awareness.

The table below explains the eight information classification labels to be used at Down to Earth Training and Assessing. These labels are not listed in any hierarchy or sequence of importance. Each label is fit for purpose for its intended description. The CEO with the support of the General Manager will allocate information classification labels where these are not already identified below as examples. The colour shown in the table below must be used to highlight the classification with the Internal classification being displayed as Blue and others including Confidential, Restricted, Private and Critical displayed in Red. Some information classifications do not require display.

Information classification labels must be prominently displayed on each item of information where it is practical to do so and the need to display the classification is specified in the Information classification label rules outlined in the table below.

| Label | Description | Examples | Rules |
|---|---|---|---|
| **Public** | Information intended for public access, openly available internally and externally without restrictions. | Marketing brochures<br>Website content<br>Student Handbook | No special security measures required.<br>May be shared externally without approval. |

| Label | Description | Examples | Rules |
|---|---|---|---|
| **Internal Only** | Information available only to Down to Earth Training and Assessing employees or approved partners and not intended for public dissemination. | Policies and procedures<br>Meeting minutes<br>Internal correspondence<br>Continuous improvement records | Distribute internally or to authorised partners only.<br>Not for public disclosure without approval.<br>Must be displayed on the information. |
| **Academic** | Information created specifically for training, learning, or assessment purposes within or associated with Down to Earth Training and Assessing. | Training manuals<br>Course handbooks<br>Assessment guidelines and resources<br>Student workbooks and learning activities<br>Training and assessment strategies | Distribute to students and trainers.<br>May be shared externally with authorisation.<br>Not intended for unrestricted public dissemination unless explicitly approved. |
| **Confidential** | Information that, if disclosed externally, could negatively impact business operations, reputation, or competitive advantage. | Business plan<br>Financial performance information<br>Contractual agreements | Limit access to need-to-know basis.<br>Secure storage and handling required.<br>External sharing needs explicit authorisation.<br>Must be displayed on the information. |
| **Restricted** | Highly sensitive business information that could lead to serious financial, legal, or reputational damage if improperly disclosed. | Legal advice or litigation information<br>Critical intellectual property<br>Business sale information | Access restricted to explicitly approved personnel.<br>Secure encryption required using BitLocker<br>No external sharing without CEO authorisation.<br>Must be displayed on the information. |
| **Private** | Personal or sensitive staff or student information protected by privacy laws and internal policies. | Student personal information<br>Staff personal information<br>Payroll information<br>Student or employer payment details | Compliance with privacy laws.<br>Restricted access only to those who need to access to perform their duties.<br>Secure storage, transmission, and disposal required. |

| Label | Description | Examples | Rules |
|---|---|---|---|
| | | | Must be displayed on the information. |
| Critical | Information vital for the ongoing operations, continuity, and stability of the business. Its loss or compromise could severely impact operations. | Business continuity plans<br>Critical infrastructure documentation<br>Insurance records<br>Administrator security credentials | Secure storage with regular backups.<br>Limited access to authorised personnel.<br>Regular integrity checks/audits.<br>Must be displayed on the information. |
| **Regulatory** | Information required by law, regulations, industry standards, or compliance frameworks. Disclosure, handling, or storage governed externally. | Records that show compliance with standards<br>Financial viability information<br>Work health and safety records | Comply fully with relevant regulations.<br>Regular audits and monitoring.<br>Clear recordkeeping and accountability required. |

## 4. Considerations

None.

## 5. Procedure

This policy is supported by procedures located within other policies:

- For procedures relating to the handling of student information on the completion of their enrolment, refer to *PP1.13 - Student Completion and Issuing Certificates.*
- For procedures relating to the handling and retention of student records, refer to *PP1.14 - Student Record Retention and Management.*
- For procedures relating to the handling of student information at the point of enrolment, refer to *PP2.2-Enrolment.*
- For procedures relating to the handling of student information in supporting the student's wellbeing, refer to *PP2.4-student Support and Wellbeing.*
- For procedures relating to student behaviour misconduct management, refer to *PP2.7-Behaviour Misconduct.*
- For procedures relating to complaint handling, refer to *PP2.9-Complaints Handling.*
- For procedures relating to appeals handling, refer to *PP2.10-Appeals Handling.*
- For procedures relating to the collection, use and disclosure of personal information during workforce recruitment, refer to *PP3.1- Workforce Planning, Recruitment and Induction.*
- For procedures relating to the management of information of trainer credentials, refer to *PP3.2-Trainer Credential Requirements.*
- For procedures relating to Information handling during staff performance management, refer to *PP3.5-Performance Management.*
- For procedures relating to mandatory information disclosure, refer to *PP4.9-Reporting Obligations.*

# 6. Other information to consider with this policy

## Policies

- PP1.13 - Student Completion and Issuing Certificates.
- PP1.14 - Student Record Retention and Management.
- PP2.2 - Enrolment.
- PP2.4 - Student Support and Wellbeing.
- PP2.7 - Behaviour Misconduct.
- PP2.9 - Complaints Handling.
- PP2.10 - Appeals Handling.
- PP3.1 - Workforce Planning, Recruitment and Induction.
- PP3.2 - Trainer Credential Requirements.
- PP3.5 - Performance Management.
- PP4.9 - Reporting Obligations.

## Forms

None.

## Handbooks, manuals or other information

None.

## 7. Flow chart

None.

## 8. Reference(s)

Compliance Standards for RTOs, Requirement 20,

- The RTO must comply with all applicable Commonwealth, State and Territory laws, including, for example, by ensuring:
  - Personal information is collected, used and disclosed by the organisation in accordance with all applicable privacy laws; and
  - The organisation complies with all applicable requirements under the Student Identifiers Act 2014.

Privacy Act 1988 (Commonwealth)

Australian Privacy Principles outlined in Schedule 1 of the Privacy Amendment (Enhancing Privacy Protection) Act 2012

Student Identifiers Act 2014

Signed & Endorsed by Managing Director

Mr Kim Brunswick:.....

Date: 25/09/2025