Privacy Protection

Relevant standard: Compliance Standards for Registered Training Organisations (RTOs), Standard 20.

Bant Training is a Registered Training Organisation with responsibility for delivering vocational education and training. Bant Training collects and stores personal information on our learners and industry clients. Bant Training complies with the Privacy Act 1988 (Commonwealth). This policy describes how Bant Training collects, manages, uses, discloses, protects, and disposes of personal information in accordance with the thirteen Australian Privacy Principles (APPs) outlined in Schedule 1 of the Privacy Amendment (Enhancing Privacy Protection) Act 2012.

Definitions

Under the Privacy Act 1988 and Privacy Amendment (Enhancing Privacy Protection) Act 2012 (s6(1)), personal and sensitive information is defined as follows:

- Personal information: "information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not."
- Sensitive information: "(a) information or an opinion about an individual's: (i) racial or ethnic origin, or (ii) political opinions, or (iii) membership of a political association, or (iv) religious beliefs or affiliations, or (v) philosophical beliefs, or (vi) membership of a professional or trade association, or (vii) membership of a trade union, or (viii) sexual preferences or practices, or (ix) criminal record, that is also personal information; or (b) health information about an individual; or (c) genetic information about an individual that is not otherwise health information; or (d) biometric information that is to be used for the purposes of automated biometric verification or biometric identification; or (e) biometric templates".

Authority to collect and store information

Bant Training is an approved Registered Training Organisation by the Australian Skills Quality Authority. This registration is issued under the authority of the National Vocational Education and Training Regulator Act 2011. This legislation requires Bant Training to collect personal and sensitive information from its learners. This requirement is specified in the Data Provision Requirements 2020 which is one of five legislative instruments that Bant Training must comply with as a condition of its registration.

The date provision requirements require Bant Training to collect data from learners in accordance with the Australian Vocational Education and Bant Training Information Statistical Standard (AVETMISS). This is a complex information standard that defines information about who the learner is, where the training is delivered and what they are studying. The Standards for Registered Training Organisations require Bant Training 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 Bant Training 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 Bant Training.

Together these requirements form a statutory obligation to collect, store and report information of any learner participating in nationally accredited training. The publications referred to in this section can be accessed from the ASQA website.

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, Bant Training 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), Bant Training may also need to report personal information to other relevant Government or responsible agencies. Students enrolling into a course with Bant Training are advised of our collection and use of personal information with the *Student Handbook* sections related to "*Your Privacy*" and "*National VET Data Policy*".

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 information collected training activity, Bant Training 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.

Collection methods

Learner personal and sensitive information as well as training activity information is prescribed by the AVETMIS Standard. This information is collected directly from our learners using enrolment forms which may be paper based or electronic and other administrative forms including but not limited to complaint forms, recognition application, request for refund, transfer application, etc. Much of this information is entered into our learner management system. Hard copy records are retained within our learner files.

Survey responses are collected using our Employer and Learner Satisfaction Surveys which are issued both in hard copy and electronic format. These survey results are returned to the main office and entered into our survey analysis software "Satisfaction Data". Survey forms once entered into Satisfaction Data are either destroyed if hard copy or permanently deleted if in electronic form.

Enquiry information from prospective learners including personal contact information is collected directly from individuals who make data requests either by telephone or email in person or via our website.

Bant Training personal information is collected from individuals on employment commencement.

Sensitive information

Personal information collected by Bant Training 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 Bant Training employees for HR management purposes.

Direct marketing

Bant Training 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. Bant Training 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 Bant Training practice to 'cold call' for the purpose of marketing its products and services. Bant Training is not to undertake in unsolicited marketing practices, ever.

Google Analytics and cookies

Google Analytics is a web service provided by Google Inc. Cookies are used to generate data on website activity and usage. The cookies, which include IP addresses, are transmitted to and stored in Google servers in the United States where they are used to compile web-use reports. Google may transfer this information to third parties, where required by law, or for information processing on its behalf. Google will not associate IP addresses with any other data held by Google. More information on Google's privacy policy can be found at: https://www.google.com.au/intl/en/policies/privacy/. It is possible to disable cookies by adjusting web-browser setting and to opt-out of Google Analytics (https://tools.google.com/dlpage/gaoptout). Doing so, however, may affect web-site functionality.

The Bant Training web servers automatically log information such as server address, date and time of visit and web pages accessed. No personal information is recorded. These logs are used for website management and improvement.

Unsolicited personal information

If Bant Training should receive unsolicited personal information, it will be treated and managed according to the Australian Privacy Principles.

Notification of collection

Bant Training 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 for telephone help-desk services, or research conducted by telephone interview.

- 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 Bant Training marketing communications.
- Quality Indicator surveys – notification is provided in the letter of invitation to participate in the surveys and also at the time of collecting the information (online or by telephone).
- Bant Training staff – Notification is provided on employment commencement.

Disclosure of personal information

Bant Training does not 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.

Bant Training may share personal information with the Commonwealth government in accordance with Commonwealth contractual obligations. In these circumstances, Bant Training 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.

Bant Training does not sell its mailing lists to third parties for marketing purposes.

Bant Training does not disclose personal information to overseas recipients. While people around the world can access material published on our website, no statistical or research publications contain identifiable personal information.

Management of personal information

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

Access to and correction of personal information

Individuals may, subject to the exceptions prescribed by the Australian Privacy Principles, request access to and correction of their personal information where this is collected directly from individuals by Bant Training.

Bant Training does not charge for giving access to or for correcting personal information. Requests for access to or correction of personal information should be made in accordance with the access to records arrangements outlined in the Learner Handbook.

Retention and recording of high risk personal information

In accordance with the *APPs principles 11.2* and *Student Identifiers Act 2014*, section 11, Bant Training 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), Bant Training is to destroy through shredding or permanently deleting these records so that these records are no longer being stored by Bant Training. Bant Training'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.

Bant Training 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.

Information security

Bant Training 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 Bant Training 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 Office 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**. Bant Training 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 Bant Training must be encrypted to ensure privacy and confidentiality. This includes data stored within student management systems. Bant Training must verify with third party suppliers of student and learning management systems that the Bant Training 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. Bant Training 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**. Bant Training 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 Bant Training.

i) **Website security**. Bant Training'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 Bant Training 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.

Information classification labels

Bant Training 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 Bant Training 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 Bant Training. 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 Office 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 Website content Student Handbook	No special security measures required. May be shared externally without approval.
Internal Only	Information available only to Bant Training employees or approved partners and not intended for public dissemination.	Policies and procedures Meeting minutes Internal correspondence	Distribute internally or to authorised partners only. Not for public disclosure without approval. Must be displayed on the information.

Label	Description	Examples	Rules
		Continuous improvement records	
Academic	Information created specifically for training, learning, or assessment purposes within or associated with Bant Training.	Training manuals Course handbooks Assessment guidelines and resources Student workbooks and learning activities Training and assessment strategies	Distribute to students and trainers. May be shared externally with authorisation. 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 Financial performance information Contractual agreements	Limit access to need-to-know basis. Secure storage and handling required. External sharing needs explicit authorisation. 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 Critical intellectual property Business sale information	Access restricted to explicitly approved personnel. Secure encryption required using BitLocker No external sharing without CEO authorisation. Must be displayed on the information.
Private	Personal or sensitive staff or student information protected by privacy laws and internal policies.	Student personal information Staff personal information Payroll information Student or employer payment details	Compliance with privacy laws. Restricted access only to those who need to access to perform their duties. Secure storage, transmission, and disposal required. 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 Critical infrastructure documentation Insurance records	Secure storage with regular backups. Limited access to authorised personnel. Regular integrity checks/audits.

Label	Description	Examples	Rules
		Administrator security credentials	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 Financial viability information Work health and safety records	Comply fully with relevant regulations. Regular audits and monitoring. Clear recordkeeping and accountability required.