BADT POL-18
Privacy & Data Storage Policy

1. **Purpose**

The purpose of this Privacy Policy is to ensure that the BADT meets its legal and ethical obligations regarding the collection, storage, use, and disclosure of personal information about individuals, companies, and other stakeholders.

This policy aligns with the Privacy Act 1988 (Cth), including the Australian Privacy Principles (APPs), the Student Identifiers Act 2014, the National VET Data Policy, the Privacy and Responsible Information Sharing Act 2024 (WA) where it applies to BADT as a contracted service provider to a Western Australian public entity, and reflects obligations under the Notifiable Data Breaches (NDB) scheme.

BADT is committed to protecting privacy, maintaining the security of personal information, and ensuring compliance with the Standards for RTOs 2025.

2. **Scope**

This policy applies to:

- Directors and Board Members
- Authorised personnel and Trainers and Assessors

- Contractors, and third-party service providers that hold or access personal information on BADT's behalf

3. **Guiding Principles**

BADT commits to:

- Collecting personal information only where necessary for our functions and activities, or as required by law.
- Informing individuals why and how their information is collected.
- Using fair and lawful means to collect personal information, obtaining consent where required.
- Protecting personal information from misuse, interference, and loss, and from unauthorised access, modification, or disclosure.
- Not disclosing personal information to third parties unless authorised or required by law.
- Notifying affected individuals and the Office of the Australian Information Commissioner (OAIC) of eligible data breaches.

- Providing clear avenues for individuals to access and correct their personal information.
- Ensuring third-party service providers comply with privacy obligations.
- Managing personal information in accordance with the National VET Data Policy and AVETMISS reporting requirements.
- Collecting, verifying, and using Unique Student Identifiers (USIs) in compliance with the Student Identifiers Act 2014.
- Seeking consent for any use of personal information in marketing materials or promotions (e.g., photos, testimonials).

4. Collection of Personal Information

BADT encourages individuals to upload all personal information direct to their personal profile via the BADT website unless unreasonable or impracticable. This includes:

- Enrolment applications
- Identification documentation
- Workplace assessments and training records

Types of information collected:

- Personal and contact details
- MDL number and expiry date
- Unique Student Identifier (USI)

Consent is obtained for the collection of sensitive information via application form and BADT website client profile, except where exemptions apply.

Heavy vehicle practical driving assessment forms issued by the Department of Transport and Major Infrastructure (DTMI) capture a health and medical declaration and eyesight result. This is sensitive information. It is collected on DTMI's form, under DTMI's privacy statement, and handled only for the purpose of the assessment.

BADT collects and reports personal information as required under the National VET Data Policy and AVETMISS for regulatory reporting to the National Centre for Vocational Education Research (NCVER) and relevant funding bodies.

Personal information is held in Australia. The third-party systems that hold personal information on BADT's behalf, and the location of their data, are listed in section 8.

5. **Use of Personal Information**

BADT uses personal information to:

- Manage course enrolments
- Verify DTMI eligibility
- Verify and manage USI
- Comply with legal and regulatory obligations
- Report training activity in accordance with the National VET Data Policy and AVETMISS

BADT honours the right of members and stakeholders to opt out of marketing communications at any time.

Where personal information is collected for use in marketing materials or promotional activities (including photographs or testimonials), informed consent is obtained prior to use.

6. **Disclosure of Personal Information**

BADT will not disclose personal information without consent, unless:

- Required by law
- Necessary to prevent a serious threat to life, health, or safety
- Permitted under this policy

BADT may share student information with:

- Registered training authorities
- Industry licensing bodies
- NCVER and funding bodies, in compliance with the National VET Data Policy

Student records provided by, or created for, a customer organisation (for example a TAFE or employer) are treated as that customer's confidential information. They are accessed only by staff who need them to deliver the training and are not disclosed to anyone else without the customer's written approval, unless required by law.

BADT will never sell or rent stakeholder information for commercial gain.

7. **Data Security and Storage**

BADT stores personal information securely:

- Electronically in systems managed under BADT's information security arrangements, as set out below
- Physically in secure locations

Only authorised staff and service providers have access to personal information, on a need-to-know basis. Access is removed when a person leaves BADT or no longer needs it.

BADT's electronic systems are managed by ACS Technology Pty Ltd and are aligned to the Australian Cyber Security Centre's Essential Eight at Maturity Level One. The controls in place are:

- Multi-factor authentication on all accounts with access to personal information, including email, the student records system and remote access
- Security patches applied to servers, devices and applications within defined timeframes: critical vulnerabilities in internet-facing systems within 48 hours, and office, browser, email and PDF applications within two weeks
- Managed endpoint protection on every BADT computer and laptop, with email filtering for malicious content
- Encryption of personal information in transit and at rest, and full-disk encryption on laptops used away from the office
- Daily backups held at a separate location, with restore testing
- Firewall protection with no direct internet access to internal systems; administrative access only through a dedicated, multi-factor protected management path
- Regular external vulnerability scanning of internet-facing systems, with findings remediated
- Logging of administrative and system access

Record retention:

- MDL & 2nd form of ID: posted weekly to DTMI

- Student MDL details, identification documents and stored payment card details: removed from the student records system automatically after 12 months of client inactivity

- Student assessment evidence: 5 years post-completion
- AQF certification documentation and attainment records: minimum 30 years (as per regulatory requirements)

Any information processed outside BADT or offsite must comply with this policy and maintain confidentiality.

At the end of its retention period, personal information is securely destroyed: paper records are shredded and electronic records are deleted so that they cannot be recovered. Where a customer organisation requests the return or destruction of its records, BADT returns or destroys them and confirms in writing when this is done.

8. Third-Party Service Providers

BADT uses the following third-party systems to hold or process personal information. Each provider is required to protect personal information to at least the standard in this policy.

- BookingTimes (Elite Design Software Pty Ltd, Brisbane) – student bookings, enrolment records, identification documents and payments. Hosted in Australia. Independently audited under SOC 2 Type II and assessed as a PCI DSS Level 1 Service Provider.
- Microsoft 365 – email, calendar and document storage. Hosted in Microsoft's Australian data centre region.
- ACS Technology Pty Ltd (Leeming, WA) – managed IT services, including servers, backup, security monitoring and incident response for LN Price & Partners Pty Ltd.

BADT does not use any service or third party where personal information is held in, or accessible from, a country outside Australia. Any new provider must be approved by the Managing Director and added to this section before personal information is placed with it.

9. Access and Correction

Individuals can access and request correction of their personal information by contacting the BADT at **bookings@badt.com.au.**

Requests will be verified (e.g., photo ID). Records will be provided within ten business days. No charge applies for access, though fees may apply for physical copies.

If information is incorrect, BADT will promptly correct it and confirm the update.

10. Data Breach Notification

A data breach is any unauthorised access to, disclosure of, or loss of personal information, whether actual or suspected. All staff must report a suspected breach to the Manager immediately.

On becoming aware of a suspected breach, BADT will, with the support of ACS Technology:

- Contain the breach and preserve evidence
- Notify any customer organisation whose records are affected within 24 hours, or sooner where its contract requires
- Notify DTMI immediately where DTMI documentation or assessment data is affected
- Assess whether the breach is likely to result in serious harm and, if so, notify affected individuals and the Office of the Australian Information Commissioner under the Notifiable Data Breaches scheme, and from 1 January 2027 the Western Australian Information Commissioner where the Privacy and Responsible Information Sharing Act 2024 applies
- Prepare a written report on the cause of the breach, its impact and the corrective action taken

BADT will not make any public statement about a breach affecting a customer organisation's records without that customer's written approval, except where required by law.

11. Staff Training and Acceptable Use

All directors, staff, trainers and assessors with access to personal information complete privacy and cyber security awareness training when they start and at least once a year. BADT keeps a record of completion.

When handling personal information, staff must not:

- Enter personal information into any artificial intelligence tool, or use it to train such a tool
- Send personal information to a personal email address or store it in a personal cloud account or on an unmanaged device
- Share login credentials, or leave personal information unattended or in plain sight
- Photograph or copy identification documents other than as required by DTMI procedures

12. Privacy Complaints

If you have concerns about how BADT has handled your personal information, please contact manager@badt.com.au.

Complaints will be managed in accordance with the BADT Complaints & Appeals Policy.

If you are not satisfied with the response, you may escalate your complaint to the OAIC at:

- Website: oaic.gov.au
- Phone: 1300 363 992

13. Related Documents

- Constitution and By-Laws
- Complaints & Appeals Policy
- National VET Data Policy [External]

- Privacy and Responsible Information Sharing Act 2024 (WA) [External]
- ACS Technology Information Security Statement
- BookingTimes Information Security Assurance and SOC 3 Report
- DTMI Heavy Vehicle PDA Information Manual and Information Bulletin 2026-01

VERSION	DATE	CREATED/AMENDED BY	COMMENTS/AMENDMENTS	RESPONSIBLE PERSON
1	13/10/26	RTO Admin	Policy created	Mg Director
1.1	29/10/26	ACS Technology / RTO Admin	Security controls, third-party providers, breach response, staff training added (CRTAFE tender)	Mg Director