

Privacy and Personal Information POLICY



SCOPE

This policy applies to:

- Students and clients
- Volt Edge employees, contractors, representatives
- Third-party service providers handling Volt Edge personal information
- All information held in digital or physical formats

Purpose

Volt Edge is committed to managing personal and sensitive information in accordance with:

- Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs)
- Notifiable Data Breaches (NDB) Scheme under the Privacy Act
- National Vocational Education and Training Regulator Act 2011 (NVETR Act) and Data Provision Requirements
- National VET Data Policy – Minimum Privacy Notice (mandatory for RTOs)
- Student Identifiers Act 2014 (USI requirements)
- Standards for Registered Training Organisations (RTOs) 2025

This policy explains how Volt Edge collects, stores, uses, discloses, protects, corrects and manages personal information.

DEFINITIONS

(Define any acronyms, jargon, or terms that might have multiple meanings)

TERM	DEFINITION
Personal Information	Information about an identifiable individual
Sensitive Information	As defined in the Privacy Act, including health information.
USI	Unique Student Identifier required for nationally recognised training.
NCVER	VET Data custodian responsible for national VET data management

Australian Privacy Principles (APP) Requirements

Open and Transparent Management (APP 1)

Volt Edge maintains this Privacy Policy on its website. It includes:

- Types of personal information collected
- How information is collected and held
- Purposes of collection
- Mandatory disclosures
- Overseas disclosures
- Access, correction and complaint processes

Anonymity and Pseudonymity (APP 2)

Where lawful and practical, individuals may interact anonymously (e.g., general enquiries).

Identification is required where:

- Enrolment
- Certification
- Verification processes (e.g., USI)

Collection of Personal Information (APP 3, 4, 5)

Volt Edge collects personal information to:

- Deliver training and assessment
- Verify student identity
- Comply with RTO regulatory reporting
- Issue qualifications
- Improve training quality
- Maintain communication with students and clients

Types of information collected

- Name, DOB, address, contact details
- Education/training history
- Employment details (where relevant)
- Payment and billing information
- USI and identity evidence
- AVETMISS-required data

Collection methods

Information is collected via:

- Application/enrolment forms
- Online portals
- Email, phone or face-to-face
- Government systems (e.g., USI Registry)
- Employers (when authorised)



Indirect collection

Volt Edge may collect information from:

- Employers
- Government departments
- NCVER data processes
- Funding bodies

Unsolicited Information (APP 4)

Unsolicited information is destroyed or de-identified unless legally required.

Collection Notice (APP 5)

At enrolment, Volt Edge provides the **National VET Data Policy – Mandatory Privacy Notice**, which:

- Identifies Volt Edge
- States the purpose of collection
- Outlines consequences of not providing information
- Explains mandatory disclosures to NCVER, DEWR, state authorities
- Provides access, correction and complaint rights
- States overseas disclosure circumstances

Use and Disclosure of Information (APP 6, 7, 8, 9)

Volt Edge uses information to:

- Enrolment, training, assessment, certification
- VET compliance and reporting
- Quality assurance and auditing
- Communication of essential training information

Mandatory RTO Disclosures

Volt Edge is required by law to disclose information to:

- NCVER (national VET data collection)
- VET regulators, DEWR, state/territory training authorities
- Other agencies where authorised under legislation

Employer - funded or co-funded training

Where training is employer-funded/co-funded, Volt Edge may provide:

- Training progress
- Assessment outcomes
- Completion records

Only with the student's written consent via the Authority to Release Information Form.

Third-party disclosures

Information may be disclosed to:

- Student Management System providers
- Payment processors
- Auditors



- IT service providers

All suppliers operate under confidentiality and privacy agreements.

USI Information

Volt Edge handles USI information in accordance with the Student Identifiers Act, including:

- Obtaining written consent before creating/verifying a USI
- Securely storing identity documents
- Limiting access to authorised staff

Direct Marketing (APP 7)

Volt Edge send promotional materials with consent. Opt-out options are provided in every communication.

Overseas Disclosures (APP 8)

Volt Edge may disclose information to cloud or system providers located in:

- List countries (or state “no overseas disclosures” if applicable)

Volt Edge ensures reasonable steps are taken to protect information to APP-equivalent standards.

Government-Related Identifiers (APP 9)

Volt Edge does not adopt government identifiers (e.g., USI) as its own.

USI INFORMATION HANDLING

Volt Edge complies with the Student Identifiers Act 2014, including:

- Obtaining written consent before creating or verifying a USI
- Secure management of identity documents
- Restricted access to authorised staff only

Data Quality and Security (APP 10 & 11)

Volt Edge takes reasonable steps to ensure accuracy of information, including:

- Regular verification of student details
- Updates upon request

Security measures include:

- Strong passwords, MFA
- Data encryption and SSL technology
- Role-based access control
- Secure destruction of records
- No permanent storage of credit card details
- Secure physical storage

The Managing Director oversees security compliance and system integrity.



Access and Correction (APP 12 & 13)

Individuals may request access or correction by emailing:

 training@voltedge.com.au

Volt Edge will:

- Respond within 30 days
- Verify identity
- Provide reasons if access is refused, as permitted by law

Notifiable Data Breaches (NDB Scheme)

A data breach occurs where personal information is lost, accessed or disclosed without authorisation.

Volt Edge will:

- Investigate within 30 days
- Notify the OAIC and affected individuals if serious harm is likely
- Record incidents in the Data Breach Register

The Managing Director coordinates breach responses.

COMMUNICATIONS

Volt Edge uses personal information to send:

- Enrolment updates
- Training notifications
- Account information

Promotional material is sent only with consent. Opt-out is available anytime.

Volt Edge complies with the **Spam Act 2003 (Cth)**

LINKS TO EXTERNAL SITES

Volt Edge is not responsible for external site content or privacy practices.

Complaints

To lodge a privacy complaint, contact:

Email: training@voltedge.com.au

If unsatisfied, individuals may escalate to the Office of the Australian Information Commissioner (OAIC):

<https://www.oaic.gov.au> | 1300 363 992

Review

This policy is reviewed annually or sooner if required by regulatory changes.

LEGISLATIVE REFERENCES

- Privacy Act 1988 (Cth)
- Australian Privacy Principles (APPs)
- NVETR Act 2011 (Cth)
- Standards for RTOs 2025



- National VET Data Policy
- Student Identifiers Act 2014
- Spam Act 2003 (Cth)

VERSION HISTORY				
VERSION	APPROVED BY	REVISION DATE	DESCRIPTION OF CHANGE	AUTHOR
1	HR & Compliance Manager	20.10.2022	Policy creation	Kirsty Brunner
1.1	Compliance Manager	13.10.2025	Updated for standards	Kirsty Brunner
1.2	Compliance	10.2.2026	Review and update for standards	Kirsty Brunner

DOCUMENT CONTROL

Document Name:	Privacy and Personal Information Policy v1.3
Author:	Kirsty Brunner
Approved By:	
Approval Date:	13.10.2025
Review Date:	13.10.2026