



Privacy Policy

Policy number	P-43		
Version number	2.0		
Drafted by	CEO		
Responsible person CEO	Mark Favetta	Signature 	Date: 26/4/22
Approved by the Board			
On behalf of the Board	Ian Fisher Board President	Signature 	Date: 26/4/22
Scheduled review date	December 2024		

Basic Beliefs/Purpose

This policy documents how Diamond Valley Learning Centre (DVLC) will collect and manage the personal and health information of its staff, students, volunteers, Board members and other individuals.

Scope

This policy applies to all DVLC staff, Board members, volunteers, contractors, and past, current or prospective students or participants.

Policy Guidelines

DVLC is committed to protecting the privacy of its employees, students, participants, volunteers and Board members as required under State and Commonwealth privacy legislation. As part of its operations, DVLC collects personal and health information by legal and fair means in order to provide efficient and effective education services. DVLC adheres to the ten Information Privacy Principles (IPPs) within Victorian privacy legislation and the thirteen Australian Privacy Principles (APPs) which form part of Commonwealth privacy legislation (refer Definitions below).

Collection

DVLC collects personal information through application / enrolment forms, in conversation, by email or through our website. Personal information, including sensitive information, collected from students may include:

- name;
- physical and mailing addresses;
- telephone numbers, including emergency contact details;
- email addresses;
- date and country of birth;
- gender;
- employment status;
- passport and / or visa information;
- disability and health information;
- languages spoken;
- school and other qualifications attained;
- Victorian Student Number (VSN) and Unique Student Identifier (USI);
- indigenous status;
- emergency contact details;
- photographic ID;
- Medicare card number;
- Driver's license number;
- Concession card details.

Personal information, including sensitive information, collected from staff members and volunteers may include:

- tax file number;
- emergency contact details;
- VIT Registration;
- Working with Children Clearance;
- Police check;
- Super Fund details;
- verified copies of qualifications.

In certain circumstances, DVLC may collect sensitive information as required by law or with consent (including the consent of parents or guardians) to assist in understanding and providing for student needs. Where possible, DVLC will collect personal information directly from the individual, but information may also be received from third parties such as government agencies or referees.

When collecting information, DVLC will take reasonable steps to advise the purpose for which information is being collected. In general, personal information is collected for the purposes of:

- providing information about our services;
- providing our education and other services;

- keeping our records up to date;
- improving our services;
- reporting to government authorities;
- complying with legal obligations;
- communicating with staff and students;
- providing an email address / login;
- direct marketing (where consented to);
- verifying Victorian Student Numbers (VSN) and Unique Student Identifiers (USI);
- addressing a complaint or appeal.

Use and Disclosure

Information collected will be used primarily in providing our services and will not be offered or sold to a third party without consent, unless in an emergency situation. Where legally required, DVLC will pass on information to Government agencies.

Sensitive information will be used and disclosed only for the purpose for which it was provided or a directly related secondary purpose, unless otherwise agreed, or the use or disclosure of the sensitive information is allowed by law.

DVLC will directly communicate marketing information to current and past students **only where consent is provided**. Communication will generally be by email, SMS or telephone, and will not contravene Australian Consumer Law. Students may opt out of this service at any time by contacting reception on 9435 9060.

Data Quality and Security

DVLC endeavours to keep its personal information records accurate and up to date at all times, and encourages staff, students and participants to notify information updates as soon as possible. All data, whether electronic or in paper format is securely protected from misuse, loss, unauthorised access or modification, and disclosure. All electronic data is backed-up regularly in case of an IT or other failure.

Access to personal information is restricted to those staff members who need to know the information in order to deliver our services. DVLC will retain all personal information as required by law or contractual obligation and will destroy or de-identify any personal information that is no longer required.

Access and Correction

DVLC recognises that people have a right to access information that we have collected from them, and to make corrections if it is incomplete, inaccurate, misleading or out-of-date. Please contact our Privacy Officer on 9435 9060 or email courses@dvlc.org.au to access or correct your personal information, or request further information.

Proof of identity is required when requesting or correcting personal information so that we can maintain security and confidentiality. DVLC will take reasonable steps to ensure that your personal information is correct, accurate, up to date, and not misleading.

Unique Identifiers

DVLC uses unique identifiers (such as a VETtrak enrolment number) for the internal administration of staff and student records, and for communication purposes. DVLC also uses government-related unique identifiers such as USI and VSN, as required under law. DVLC will not disclose unique identifiers to an outside organisation unless required to do so by law or obligated under government contracts.

Transborder Data Flow

DVLC reports your information to the State Training Authority, and/or to Commonwealth Government agencies under law and does not, in general, transfer your information outside of Australian borders. DVLC may use IT platforms such as cloud computing services or Google Docs to store your personal information on servers which are generally located outside of Australia.

Anonymity

DVLC respects an individual's right to anonymity, except in circumstances where proof of identity is required. Failure to provide certain personal information may restrict DVLC's ability to offer services or provide access to government support.

Data Breaches

DVLC takes all data breaches seriously and will investigate the circumstances of loss, damage, unauthorised access or disclosure and other breaches of personal information. Staff members must report all suspected breaches to the Chief Executive Officer (CEO).

The CEO will use objective measures to determine the seriousness of the breach. This may include reviewing the type and sensitivity of the information, the persons involved, how long ago the breach occurred, the likelihood of identity theft, the likely impact on an individual's financial security, personal or psychological safety, potential reputational damage, and the extent and effectiveness of remedial action taken by DVLC.

Data breaches likely to result in serious harm to an individual such as physical, psychological, emotional, financial or reputational harm will be reported to the Office of the Australian Information Commissioner in accordance with the National Data Breaches Scheme requirements.

Complaints

If you feel that your privacy has been breached, or have any complaints about how your personal information has been handled, please contact our Privacy Officer on 9435 9060 or email courses@dvlc.org.au.

External avenues for complaint include:

Office of the Victorian Information Commissioner (OVIC)

PO Box 24274, Melbourne VIC 3001

W: <https://ovic.vic.gov.au/>

E: enquiries@ovic.vic.gov.au

T: 1300 006 842 (1300 00 OVIC) between 9am and 5pm, Monday to Friday.

Office of the Australian Information Commissioner (OAIC)

GPO Box 5218, Sydney NSW 2001

W: www.oaic.gov.au

E: enquiries@oaic.gov.au

T: 1300 363 992 Mon–Thurs 10am–4pm AEST/AEDT

Definitions

The **Australian Privacy Principles** are a set of legally binding national standards for handling, holding, accessing and correcting personal information. The full text can be found at Schedule 1 of the Privacy Act 1988

- Australian Privacy Principle 1 – open and transparent management of personal information
- Australian Privacy Principle 2 – anonymity and pseudonymity
- Australian Privacy Principle 3 – collection of solicited personal information
- Australian Privacy Principle 4 – dealing with unsolicited personal information
- Australian Privacy Principle 5 – notification of the collection of personal information
- Australian Privacy Principle 6 – use or disclosure of personal information
- Australian Privacy Principle 7 – direct marketing
- Australian Privacy Principle 8 – cross-border disclosure of personal information
- Australian Privacy Principle 9 – adoption, use or disclosure of government related identifiers
- Australian Privacy Principle 10 – quality of personal information
- Australian Privacy Principle 11 – security of personal information
- Australian Privacy Principle 12 – access to personal information
- Australian Privacy Principle 13 – correction of personal information

A **data breach** is the unauthorised access, disclosure or loss of personal information held by an organisation. Examples of a data breach include a lost or stolen device containing personal information, or mistakenly providing personal information to the wrong person.

Health information is information or opinion about a person’s physical, mental or psychological health, or disability, health status or medical history, whether recorded or not.

The **Information Privacy Principles** set out the minimum standards under which Victorian public sector and publicly funded organisations manage personal information. The full text can be found at Schedule 1 of the Privacy and Data Protection Act 2014 (Vic)

- Principle 1 – Collection
- Principle 2 – Use and Disclosure
- Principle 3 – Data Quality
- Principle 4 – Data Security
- Principle 5 - Openness
- Principle 6 – Access and Correction
- Principle 7 – Unique Identifiers
- Principle 8 - Anonymity
- Principle 9 – Transborder Data Flows
- Principle 10 – Sensitive Information

A **Notifiable Data Breach (NDB)** is the legal obligation under the Privacy Act 1988 for organisations to report all data breaches that are likely to result in serious harm to one or more individuals, to the Australian Information Commissioner.

Personal information is defined in s 6(1) of the Privacy Act, as information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable.

It includes a broad range of information such as name, address, telephone number, email address, photographs, bank account details, assessment results, gender, marital status and parent/guardian details.

Sensitive information is personal information that includes information or an opinion about an individual's racial or ethnic origin, political opinions or associations, religious or philosophical beliefs, trade union membership or associations, sexual orientation or practices; criminal record, health or genetic information; and some aspects of biometric information. Generally, sensitive information has a higher level of privacy protection than other personal information.

Related Policies

- P-8 Student Welfare and Duty of Care Policy
- P-13 Code of Conduct and Ethics Policy
- P-14 Accuracy and Integrity of Student Records Policy
- P-16 Student Complaints and Appeals Policy and Procedure
- P-19 Records Management and Archive Policy
- P-21 Accuracy and Integrity of Marketing Policy
- P-26 Access, Anti-Discrimination, Equity, Diversity and Empowerment Policy
- P-35 Mandatory Reporting Policy
- P-42 Consumer Protection Policy
- P-44 Student Engagement Policy
- P-59 Computers, Internet and Email Policy and Procedure
- P-60 Social Media Policy and Procedure

Related Documents

- D-015 Data Breach Response Plan
- F-009 Enrolment Form
- F-012 Incident Report Form
- F-035 Complaints and Appeals Form
- F-073 Request for Student Results Form
- F-121 Student Credit Transfer Application Form
- F-122 Student RPL Application Form
- F-131 Permission to Provide Contact Details
- Pre-Training Interviews
- Skills First Quality Charter

Mapping Information

- AQTF Condition 3
- AQTF Standard 2
- VRQA VET Provider Guideline 2

Legislation and Regulation

- Charter of Human Rights and Responsibilities Act 2006 (Vic)
- Child Wellbeing and Safety Act 2005 (Vic)
- Children, Youth and Families Act 2005 (Vic)
- Consumer and Competition Act 2010
- Education and Training Act 2006 (Vic)
- Health Records Act 2001 (Vic)
- Privacy Act 1988
- Privacy and Data Protection Act 2014 (Vic)