# Privacy Policy and Procedure

RTO No. 46394

## 1. Purpose

SDG College Pty Ltd is committed to protecting the privacy, confidentiality, and security of personal and sensitive information in accordance with applicable legislation and regulatory requirements, including the Privacy Act 1988 (Cth), Australian Privacy Principles (APPs), Student Identifiers Act 2014, Data Provision Requirements 2020, and the Standards for Registered Training Organisations (RTOs) 2025.

This policy establishes a comprehensive and system-based framework governing the lawful collection, use, disclosure, storage, access, retention, and disposal of personal information. It ensures that all information handled by the organisation is managed in a manner that is transparent, secure, and consistent with regulatory expectations, while safeguarding the rights and interests of students, staff, and stakeholders.

This policy directly supports **Outcome Standard 2.1**, ensuring students are properly informed, and **Outcome Standard 4.1**, ensuring organisational integrity and accountability.

## 2. Scope

This policy applies to all personal, sensitive, and high-risk personal information collected, stored, accessed, used, or disclosed by the organisation across all operational areas.

It applies to:

- all students (current, prospective, and past)
- all staff, contractors, and third parties
- all training and administrative activities
- all systems including Student Management System (SMS), AVETMISS reporting, and internal records
- all forms of information including digital, physical, and verbal

This ensures that privacy management is embedded across all organisational functions and not limited to administrative processes.

## 3. Policy Principles

SDG College adopts a structured, system-based approach to privacy management, ensuring that personal information is handled lawfully, fairly, and securely at all stages of the information lifecycle.

The organisation ensures that personal information is collected only where necessary for lawful purposes, including enrolment, training delivery, assessment, certification, regulatory reporting, and student support. Individuals are informed of the purpose and use of their information prior to or at the point of collection, ensuring transparency and informed consent.

Sensitive information is subject to enhanced safeguards, recognising the higher risk associated with such data. Access to all personal information is restricted based on role and responsibility, ensuring that only authorised personnel can access or handle such data.

The organisation applies robust security controls to prevent misuse, loss, unauthorised access, modification, or disclosure of personal information. Information is retained only for as long as required under regulatory obligations and is securely disposed of when no longer required.

Privacy practices are subject to ongoing monitoring, review, and continuous improvement to ensure alignment with evolving regulatory requirements and organisational needs.

Where lawful and practicable, individuals may interact with the organisation anonymously or using a pseudonym; however, this may not be possible where identification is required for enrolment, certification, or regulatory reporting.

**4. Collection of Personal Information**

The organisation collects personal information in a lawful and fair manner, and only where it is necessary to perform its functions as a Registered Training Organisation.

Personal information is collected:

- to process enrolments and student administration
- to deliver training and assessment services
- to provide learner support and wellbeing services
- to issue certification documentation
- to comply with regulatory and reporting requirements

**Types of Information Collected**

| Category | Examples | Purpose |
|---|---|---|
| Personal Information | Name, DOB, contact details | Identification and communication |
| Government Identifiers | USI, ID verification documents | Compliance and verification |
| AVETMISS Data | Demographics, education background | National reporting |
| Academic Records | Results, attendance | Training and certification |
| Sensitive Information | Disability, language, support needs | Learner support |

Collection is supported by legislative obligations, including AVETMISS and USI requirements.

### 5. Use and Disclosure of Personal Information

SDG College Pty Ltd ensures that personal information is used strictly for the primary purpose for which it was collected, unless the use or disclosure is otherwise required or authorised under law, including the Privacy Act 1988 (Cth).

The organisation uses personal information in a controlled and structured manner to support its functions as a Registered Training Organisation. All use of personal information is directly related to training delivery, regulatory compliance, and student support, ensuring that data handling remains lawful, transparent, and proportionate.

**Use of Personal Information**

The organisation uses personal information for the following purposes:

- delivery of training and assessment services
- provision of academic and welfare support
- maintenance of student records and progression tracking
- issuance of AQF certification documentation
- compliance with reporting obligations (e.g., AVETMISS, USI)
- communication with students regarding enrolment, progress, and outcomes

**Disclosure of Personal Information**

Personal information may be disclosed where required for lawful and operational purposes.

| Recipient | Purpose of Disclosure |
|---|---|
| **Government agencies (e.g., NCVER, ASQA)** | Regulatory reporting and compliance |
| **Authorised third parties (if applicable)** | Service delivery and operational support |
| **Regulatory / licensing bodies** | Legal and statutory obligations |

The organisation ensures that:

- personal information is not sold, rented, or traded under any circumstances
- disclosure is limited to what is necessary and proportionate
- reasonable steps are taken to ensure that third parties comply with privacy obligations
- disclosure complies with the Australian Privacy Principles (APP 6 – Use or Disclosure)

The organisation does not routinely disclose personal information to overseas recipients. Where such disclosure may occur (for example, through the use of cloud-based systems or service providers), the organisation takes reasonable steps to ensure that the recipient complies with the Australian Privacy Principles.

**6. Notification of Collection**

SDG College ensures that individuals are informed about the collection, use, and disclosure of their personal information prior to, or at the time of, collection.

Notification is provided through structured and consistent mechanisms, ensuring transparency and informed participation.

**Notification Methods**

- Student Handbook
- Student Application forms and agreements
- website privacy notices
- direct communication during enrolment or orientation

The organisation ensures that individuals are clearly informed of:

- the purpose of collection
- how their information will be used and disclosed
- any legal or regulatory requirements
- their rights to access and correct their information

Individuals are informed whether the collection of personal information is required by law or necessary to provide services.

**7. Sensitive and High-Risk Personal Information**

SDG College collects and manages sensitive and high-risk personal information in a controlled and restricted manner, recognising the increased risk associated with such data. Sensitive information is collected only where it is required under legislation, such as AVETMISS reporting obligations, or where it is necessary to provide appropriate academic or welfare support to the learner.

High-risk personal information, including identity documents such as passports or driver's licences, is handled with enhanced safeguards to ensure confidentiality, integrity, and security. The organisation ensures that such information is collected only where strictly necessary, used solely for verification or support purposes, and is accessible only to authorised personnel. Information of this nature is not retained longer than required and is securely destroyed once its purpose has been fulfilled.

The organisation adopts a "verification over storage" approach, ensuring that identity and sensitive information is validated without unnecessary retention, thereby minimising privacy risk.

RTO No. 46394

**Control Framework for Sensitive Information**

| Control Area | Measures Implemented |
|---|---|
| Collection | Limited to necessary and lawful purposes |
| Storage | Secure systems with restricted access |
| Use | Strictly limited to intended purpose |
| Disposal | Secure destruction after use |

### 8. Direct Marketing

SDG College ensures that all marketing activities are conducted in a lawful, ethical, and controlled manner. The organisation does not engage in unsolicited or misleading marketing practices and complies with the requirements of the Spam Act 2003 (Cth).

Personal information is not used for direct marketing purposes unless consent has been provided or such use is otherwise permitted under applicable legislation. Where marketing communications are issued, individuals are provided with clear and accessible opt-in and opt-out mechanisms, ensuring transparency and control over their personal information.

### 9. Data Security and Protection

The organisation applies a comprehensive and layered approach to information security to protect personal information from misuse, interference, loss, unauthorised access, modification, or disclosure. Security controls are embedded across digital, physical, and operational environments, ensuring that information is safeguarded throughout its lifecycle.

Access to personal information is strictly controlled through role-based permissions, ensuring that only authorised personnel can access sensitive or confidential data. Systems are regularly monitored and reviewed to maintain security integrity and respond to emerging risks.

Access to systems is regularly reviewed to ensure continued appropriateness of user permissions.

**Security Framework**

| Area | Key Controls |
|---|---|
| Digital Security | Secure SMS, password protection, MFA, encryption, system backups |

| Area | Key Controls |
|---|---|
| Physical Security | Locked storage, restricted premises access |
| Operational Controls | Staff training, confidentiality obligations, role-based access |
| Monitoring & Review | System audits, access logs, regular compliance checks |

The organisation takes reasonable steps to protect personal information in accordance with APP 11 – Security of Personal Information, ensuring data integrity, confidentiality, and availability at all times.

**10. Access and Correction**

SDG College recognises the right of individuals to access and correct their personal information in accordance with the Privacy Act 1988 (Cth). The organisation ensures that requests for access are handled in a timely, transparent, and secure manner.

Before granting access, the organisation verifies the identity of the individual to protect the integrity of personal information. Access to view records is provided at no cost, and requests for correction are assessed and implemented promptly to ensure that all information held is accurate, complete, and up to date.

**11. Retention and Disposal**

The organisation retains personal information only for as long as necessary to meet legal, regulatory, and operational requirements. Retention practices are aligned with legislative obligations and the organisation's Records Management Policy, ensuring that information remains accessible where required while minimising unnecessary storage.

**Retention Framework**

| Record Type | Retention Period |
|---|---|
| Certification Records | Minimum 30 years (AQF requirement) |
| Student Records | Minimum 2 years after completion or cancellation |
| Assessment Evidence | Minimum 2 years after completion or cancellation |

High-risk personal information is not retained longer than necessary and is securely destroyed once verification or processing requirements have been completed. Disposal methods include secure shredding of physical documents and secure deletion of electronic records.

**12. Data Breach and Incident Management**

SDG College maintains a structured and responsive approach to managing data breaches and privacy incidents. The organisation is committed to identifying, containing, and resolving breaches in a timely and effective manner to minimise impact and prevent recurrence.

In the event of a data breach, the organisation will identify and contain the incident, assess the nature and severity of the risk, and implement immediate corrective actions. All incidents are documented, investigated, and reviewed as part of the organisation's continuous improvement framework.

Where required, the organisation complies with the Notifiable Data Breach (NDB) Scheme, including notification to affected individuals and relevant authorities.

**13. Complaints and Privacy Concerns**

Individuals have the right to raise concerns or lodge complaints regarding the handling of their personal information. SDG College ensures that all privacy-related complaints are managed in accordance with the Complaints and Appeals Policy and in line with the principles of procedural fairness and natural justice.

Individuals are not subject to any form of victimisation, discrimination, or adverse treatment as a result of lodging a privacy complaint or concern.

All complaints are formally recorded, acknowledged, and investigated, with outcomes communicated transparently. Complaints are also used to identify systemic issues and inform continuous improvement.

Privacy-related enquiries and complaints may be directed to the organisation via the official contact details listed in the Student Handbook or website.

**14. Continuous Improvement**

Privacy management is embedded within the organisation's governance and continuous improvement framework. The organisation systematically monitors privacy practices to ensure ongoing compliance, effectiveness, and alignment with regulatory requirements.

Monitoring activities include internal audits, incident and breach analysis, governance and management meetings, and periodic review of policies and procedures. All improvement actions are documented in the Continuous Improvement Register, assigned to responsible personnel, and monitored through to completion.

The organisation applies the principle of No Close Without Verification

ensuring that all improvements are implemented, reviewed, and supported by evidence before closure.

**15. Responsibilities**

SDG College defines clear roles and responsibilities to ensure accountability and effective implementation of privacy management practices across the organisation.

# Privacy Policy and Procedure

RTO No. 46394

| Role | Responsibility |
|---|---|
| Chief Executive Officer (CEO) | Provides governance oversight and ensures compliance with privacy legislation |
| General Manager | Monitors implementation and operational compliance |
| Administration Staff | Manage data collection, storage, and record handling |
| Trainers and Staff | Maintain confidentiality and protect student information |
| All Staff | Comply with privacy obligations and report any breaches or concerns |

All staff are required to handle personal information responsibly, comply with this policy and applicable legislation, and immediately report any actual or suspected privacy breaches.