Oxford Training Academy Pty Ltd t/a Savile Learning RTO 45452

Privacy and Data Protection Policy and Procedure

Contents

Oxford Training Academy Pty Ltd trades as Savile Learning and will be referred to as Savile in this policy and procedure document.

Purpose

The purpose of this policy is to establish Savile's framework for managing personal and sensitive information in compliance with the Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs) and the Notifiable Data Breaches (NDB) scheme. It defines Savile's approach to the collection, use, storage and disclosure of information, outlines how eligible data breaches are identified, contained, assessed and notified, and sets out strategies for securing both digital and hard-copy records through appropriate classification and access controls.

Scope

This policy and procedure has been developed by Savile and applies to all personal and sensitive information collected, held, used or disclosed by Savile in the course of its operations as a Registered Training Organisation (RTO), including information about students, prospective students, employees, contractors, trainers and assessors, third parties, and industry or employer clients, whether held in hard copy or digital format. It applies to all Savile staff, contractors and third parties who collect, access, use or disclose personal information on Savile's behalf.

Policy Statement

Savile collects and stores personal and sensitive information about its students, staff and industry clients. Savile has introduced this policy to comply with its obligations under the Privacy Act 1988 (Cth) and to safeguard staff and students from potential financial or reputational harm. Mishandling personal and sensitive data can lead to breaches of trust, reputational damage, regulatory action, and loss of student and industry confidence.

The following principles underpin Savile's approach to privacy and data protection:

- Personal information is collected, used, stored and disclosed fairly, lawfully, and only for purposes connected with Savile's functions as an RTO;
- Sensitive information is only collected where reasonably necessary, with consent, or as required by law;
- Personal and sensitive information is protected from misuse, interference, loss, and unauthorised access, modification or disclosure;
- Individuals are able to access their personal information and seek correction of that information;
- Suspected and actual data breaches are contained, assessed and, where required, notified in accordance with the Notifiable Data Breaches scheme; and
- Privacy practices are monitored and continuously improved, with findings recorded in Savile's Continuous Improvement Register.

Responsibilities

- *CEO*: Overall accountability for privacy and data protection compliance, resourcing and oversight; approves this policy and any data breach notification decisions.
- *RTO Manager / Administration*: Manages day-to-day collection, storage and disclosure of student and client personal information, provides Privacy Collection Notices at enrolment, processes access and correction requests, and maintains secure filing systems.

- *Compliance Lead/Quality Team*: Maintains this policy, monitors compliance with the APPs, coordinates data breach assessment and response, maintains the record retention and disposal schedule, and refers systemic issues to the CEO.
- *IT / Systems Provider:* Implements and maintains technical security controls over digital systems, including access controls, back-up and, where available, encryption.
- *Trainers and Assessors*: Collect only the personal information necessary for training and assessment purposes, handle student information securely, and report any suspected privacy or security incident immediately.
- *All staff and contractors*: Comply with this policy, complete privacy-related training, and report suspected breaches without delay.
- *Learners*: Provide accurate information, notify Savile of changes to personal details, and may raise privacy concerns or complaints through Savile's complaints process.

Definitions

Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information is true or not. This includes name, signature, address, phone number, date of birth, employment record information, and other identifying data such as IP addresses or biometric information.

Sensitive information means personal information or opinions concerning an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, memberships of professional, trade or trade union associations, sexual orientation, criminal record, health information, or genetic or biometric information.

De-identified information means information that is no longer about an identifiable individual, or an individual who is reasonably identifiable, because identifying details have been removed.

Data breach means an event or circumstance that has resulted, or may result, in unauthorised access to, unauthorised disclosure of, or loss of, personal information Savile holds.

Eligible data breach means a data breach that is likely to result in serious harm to one or more individuals, where Savile has been unable to prevent that likely risk of serious harm through remedial action, triggering notification obligations under Part IIIC of the Privacy Act 1988 (Cth).

Third party means any organisation or individual, other than Savile and the individual concerned, that collects, holds, uses or discloses personal information on Savile's behalf or in connection with Savile's operations.

Unique Student Identifier (USI) means the identifier created under the Student Identifiers Act 2014 (Cth) that is required to be verified before Savile issues AQF certification documentation.

AVETMISS means the Australian Vocational Education and Training Management Information Statistical Standard, the national data standard RTOs must comply with for reporting student and training activity data

Collection of Personal Information

Savile collects personal information by lawful and fair means only and does not collect information in a way that is unreasonably intrusive.

Authority to Collect and Store Information

Savile is a Registered Training Organisation approved by the National VET Regulator, ASQA, under the authority of the National Vocational Education and Training Regulator Act 2011. This registration requires Savile to collect personal and sensitive information from students in accordance with the Data Provision Requirements 2020, which requires data to be collected in line with the Australian Vocational Education and Training Information Statistical Standard (AVETMISS). The Standards for RTOs 2025 require Savile to retain and report this information in accordance with mandatory reporting requirements. The Student Identifiers Act 2014 (Cth) also requires Savile to collect high-risk personal information for the purpose of creating or verifying a student's Unique Student Identifier (USI).

- What Information Is Collected
- Contact and identification details, including name, date of birth, address, phone number and email;
- Enrolment and training activity information required for AVETMISS and funding contract reporting;
- USI details, verified before certification is issued;
- Assessment records, results, and Recognition of Prior Learning applications and evidence;
- Disability status, language spoken at home, country of birth and other AVETMISS-required demographic data, where provided by the student;
- Complaints, appeals, and satisfaction survey responses;
- Staff, trainer and assessor HR information, including address, bank details, WWCC/VIT and credential records; and
- Venue access and WHS-related records, where training is delivered on third-party or client premises.

What Individuals Are Told at Collection

At or before the time personal information is collected, Savile makes individuals aware of:

- Savile's identity and how to contact it;
- the individual's right to access the personal information Savile holds about them;
- the purpose for which the information is being collected;
- the organisations, or types of organisations, to which Savile usually discloses that kind of information;
- any law that requires the particular information to be collected; and
- the consequences, if any, for the individual if the required information is not provided.

Savile's Privacy Collection Notice is included in its Application for Enrolment Form, Offer Letter and Student Agreement documentation; staff contracts of employment also refer to privacy rights and obligations.

Information Collected from Third Parties

Savile sometimes collects personal information about an individual from another person or organisation rather than directly from that individual for example, where a school or industry partner provides the name and contact details of a VET Coordinator or nominated teachers as part of arranging or auspicing VET delivery at that school, where a client is referred by a third party, or as part of a group enrolment. Where this occurs, the organisation providing the information is responsible for making the individual aware that their details have been provided to Savile and for directing them to this policy, consistent with Savile's collection notices; where practicable, Savile also contacts each individual directly to ensure they are aware of the matters set out above.

Solicited Information

Contact information such as name, organisation, position, address, phone number and email is collected for marketing, support services, mandatory reporting and day-to-day communication with stakeholders. Savile also collects, stores and reports information relating to satisfaction surveys, complaint handling, and its industry or employer clients.

Sensitive Information

Personal information collected by Savile that may be regarded as 'sensitive' under the Privacy Act includes disability and long-term impairment status, indigenous status, language spoken at home, and country of birth, where specified in AVETMISS data elements and collected for national VET data collections. Dietary requirements (health-related) may be collected for training delivery or event catering purposes only. Membership of professional or trade associations and health or work-injury information may be collected from Savile staff, trainers and assessors for HR management and credentialing purposes. Savile only collects sensitive information where the individual has given written consent, unless collection is otherwise required or authorised by law, and will only use sensitive information for the primary purpose for which it was obtained, for a directly related secondary purpose, with the individual's consent, or where required or authorised by law.

Direct Marketing

Savile respects an individual's right not to receive marketing material and provides an unsubscribe option within communications and on its website. Savile conducts its marketing communications in accordance with Australian Privacy Principle 7 (Direct Marketing) and the Spam Act 2003 (Cth).

Use and Disclosure of Personal Information

Savile will only use or disclose personal information for the primary purpose for which it was collected, a directly related secondary purpose an individual would reasonably expect, with the individual's consent, or as required or authorised by law. This includes:

- mandatory reporting to Commonwealth and, where relevant, State or Territory government agencies for AVETMISS, USI, and funding contract purposes, including disclosure of nationally recognised training data to the National Centre for Vocational Education Research Ltd (NCVER);
- disclosure to industry regulators or licensing bodies where necessary to facilitate an outcome of a service, such as licensing;

- disclosure to a third party engaged to deliver or assess training on Savile's behalf, under a written agreement requiring compliance with this policy;
- disclosure to service providers engaged by Savile to operate on its behalf, such as electronic signature platforms used to execute Auspicing Agreements and other arrangements with schools and industry partners;
- disclosure to an employer, school or industry partner that has funded or arranged a student's training, with the relevant consent;
- disclosure reasonably believed necessary to prevent or lessen a serious and imminent threat to life, health or safety; and
- disclosure required or authorised by or under law, including for law enforcement purposes.

Savile will not disclose personal information to any other person, body or agency without the individual's express or implied consent, except as set out above. Students are advised of Savile's collection and use of personal information through the Student Handbook sections on “Your Privacy” and “National VET Data Policy”.

Storage and Security of Personal Information

In line with Australian Privacy Principle 11, Savile takes reasonable steps to protect the personal information it holds from misuse, interference, loss, and unauthorised access, modification or disclosure. Security measures include:

- individual, password-protected access to Savile's systems and databases;
- secure, lockable filing cabinets and locked, access-controlled rooms for hard copy records; and
- secure storage and access-controlled office facilities.
- Digital records are stored in secure, access-controlled systems, protected by user authentication and, where available, encryption, with regular back-ups.
- Access to student and staff records is restricted to authorised personnel on a need-to-know basis.
- Devices used to access Savile's systems are password protected; portable devices and removable media containing personal information are not left unsecured.
- Personal information that is inaccurate, irrelevant or no longer needed for any purpose for which it may be used or disclosed is destroyed in a way that renders it unusable – for example, hard copy records are shredded and digital records are securely deleted or de-identified provided Savile is not required by law to retain it. The Data Provision Requirements 2020 require certain student records to be retained for up to 30 years; other records are retained in line with Savile's Records Management Policy.
- Third parties engaged by Savile must demonstrate equivalent security safeguards under a written agreement.

Data Quality

Savile takes reasonable steps to ensure that the personal information it collects, uses or discloses is accurate, complete and up to date, and updates its records promptly when notified of a change by the individual concerned.

Overseas Disclosure of Personal Information

Savile engages service providers, such as electronic signature platforms, to support its operations, and some of these providers store or process personal information on servers located outside Australia. In accordance with Australian Privacy Principle 8 (Cross-border disclosure of personal information), Savile takes reasonable steps to ensure that any overseas recipient of personal information handles that information consistently with the Australian Privacy Principles before the information is disclosed. Where a specific overseas storage or processing arrangement applies to information collected for a particular purpose, this is disclosed to the individual in the relevant Privacy Collection Notice at the time of collection.

Access, Correction and Complaints

Individuals may request access to the personal information Savile holds about them, at no cost, and may request correction of information that is inaccurate, out of date, incomplete, irrelevant or misleading. Requests are made in writing to Administration, or to info@savilerto.com.au. Savile will ask the individual to provide evidence of identity, such as a driver licence or bank card, before releasing personal information. Requests are responded to within a reasonable timeframe, generally within ten (10) business days. Savile may decline access in limited circumstances permitted under the Privacy Act and will provide reasons in writing where access is refused.

Individuals who believe Savile has breached the Australian Privacy Principles may lodge a complaint under Savile's Complaints and Appeals Policy and Procedure. If a complaint is not resolved internally, it may be referred to the Office of the Australian Information Commissioner (OAIC).

Identifiers

Savile will only assign a unique identifier to an individual such as a student's Unique Student Identifier (USI) where necessary to carry out one or more of Savile's functions or activities, or where required by law, including the Student Identifiers Act 2014 (Cth). Savile does not use or disclose that identifier other than for the purpose for which it was assigned, or as otherwise required or authorised by law, and does not adopt as its own an identifier assigned by another agency unless required by the Standards for RTOs 2025 or by law.

Data Breach Response

Savile has obligations under the Notifiable Data Breaches (NDB) scheme in Part IIIC of the Privacy Act 1988 (Cth). An eligible data breach occurs where there is unauthorised access to, or unauthorised disclosure of, personal information (or a loss of personal information likely to result in unauthorised access or disclosure), that is likely to result in serious harm to one or more individuals, and Savile has not been able to prevent that likely risk of serious harm through remedial action. Where a suspected or actual data breach occurs, Savile will:

Contain: take immediate remedial action to contain the breach and prevent further compromise of personal information.

Assess: gather the facts, identify the individuals and information affected, and assess whether the breach meets the threshold of an eligible data breach.

Notify: where the breach is assessed as an eligible data breach, notify affected individuals and the OAIC without delay, including recommended steps individuals should take.

Review: identify root causes, implement corrective and preventive actions, and record the outcome in the Continuous Improvement Register.

The CEO or delegate is responsible for determining whether a breach is an eligible data breach and for coordinating Savile's response and any required notifications.

Privacy Procedure

Step 1: Collection Notice

Savile provides a Privacy Collection Notice to students and staff at or before the point personal information is collected, explaining what is collected, why, and how it will be used, stored and disclosed, including reference to the Student Handbook.

Step 2: Enrolment and Ongoing Collection

Personal information is collected directly from the individual wherever practicable, using enrolment forms, application forms and other approved collection tools, and only where reasonably necessary for Savile's functions.

Step 3: Secure Storage

Information is filed or entered into Savile's systems promptly and stored in accordance with the security controls set out in this policy, whether in hard copy or digital form.

Step 4: Use and Disclosure Checks

Before using or disclosing personal information, staff confirm the purpose is consistent with this policy, that any required consent has been obtained, and that any third-party receiving information is bound by an appropriate written agreement.

Step 5: Access and Correction Requests

Administration reviews written requests for access to personal information, arranges for the individual to view or receive a copy of their information, updates records in line with any correction requested, and retains documentation of the request and the action taken.

Step 6: Data Breach Identification and Escalation

Any staff member who becomes aware of a suspected data breach reports it immediately to the Compliance Lead or CEO, who initiate the containment, assessment and notification steps set out under Data Breach Response.

Step 7: Retention and Disposal

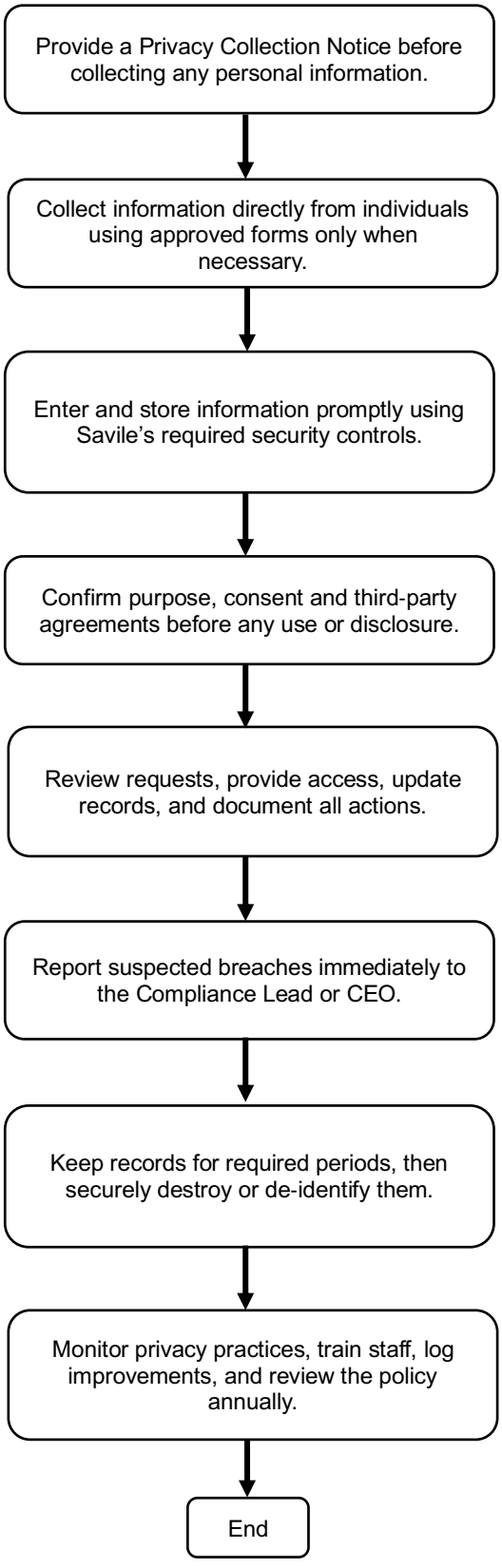
Records are retained in line with the Data Provision Requirements 2020, the Standards for RTOs 2025, and Savile's Records Management Policy, and are securely destroyed or de-identified once retention periods have expired.

Step 8: Monitoring, Training and Continuous Improvement

Savile monitors privacy practices through file reviews, complaints and breach data, provides privacy training to staff, and records findings and corrective actions in the Continuous

Improvement Register. This policy is reviewed at least annually or earlier if legislative, regulatory or operational changes require amendment.

Privacy Procedure Flowchart



References

Supporting Documents

- Privacy Collection Notice(s) – including form/purpose-specific notices such as the School / Auspicing Partner Collection Notice
- Student Handbook
- Enrolment forms
- Client, student and staff files, including academic records
- Student Management System (SMS) records
- Data Breach Response Register
- Records Management Retention and Disposal Schedule
- Access and Correction Request Form
- Continuous Improvement Register
- Complaints and Appeals Register
- Third-Party Agreements

Supporting Policies

- Records Management Policy
- Complaints and Appeals Policy and Procedure
- Student Enrolment Policy and Procedure
- USI Policy and Procedure
- Third-Party Arrangements Policy
- Information and Communications Technology (ICT) Security Policy
- Continuous Improvement and Quality Assurance Policy and Procedure

Legislative/statutory requirements

- Privacy Act 1988 (Cth)
- Australian Privacy Principles (APPs)
- Notifiable Data Breaches (NDB) scheme – Part IIIC, Privacy Act 1988 (Cth)
- Spam Act 2003 (Cth)
- National Vocational Education and Training Regulator Act 2011
- National VET Regulator (Data Provision Requirements) Instrument 2020
- National VET Data Policy
- Student Identifiers Act 2014 (Cth)

Standards

Standards for RTOs, listed below.

https://www.dewr.gov.au/revisions-standards-registered-training-organisations/resources/policy-draft-compliance-requirements

Quality Area 1 – Training and Assessment

Quality Area 4 – Governance

Compliance Requirements

The Compliance Requirements establish the Information Management obligations:

- Compliance Requirements Clause 11: RTOs must manage student and staff information and records in a secure, accurate and accessible manner, consistent with the collection, storage, security, access and retention requirements set out in this policy.

Outcome Standards for RTOs

The key Outcome Standards that directly apply to privacy and data are:

- Outcome Standard 1.5: RTOs must provide accurate and accessible information to prospective and current learners, including how their personal information is collected, used and disclosed, consistent with Savile's Privacy Collection Notices and the Student Handbook.
- Outcome Standard 4.2: RTOs must meet their compliance and regulatory reporting obligations, including the accurate reporting of student data to government agencies (AVETMISS, USI, NCVER) in accordance with this policy.
- Outcome Standard 4.3: RTOs must maintain effective governance risk-management systems, including identifying and managing privacy and data security risks and responding to incidents such as data breaches.

Version Control

Version	Date	Changes / Updates	Approved by
1.6			CEO
2.0	12/08/2026	New policy developed for Savile, replacing prior informal privacy arrangements, aligned to the Standards for RTOs 2025.	

Review Date: August 2027