

Privacy Policy		Policy Number: SCAP0027 Date of Issue: 02/10/2026 Review Date: 02/10/2027 RTO Code: 41267	
		Authorised by: Managing Director	Issued to: Public, RTO staff & students
		Pages: 7	Version: 2.0

1. Purpose

Star College Australia Pty. Ltd. (SCA) is committed to managing personal information openly, transparently and securely. This policy explains how SCA collects, holds, uses and discloses personal information, how individuals may access or correct their information or make a privacy complaint and how SCA meets its privacy, VET reporting and recordkeeping obligations.

This policy is intended to operate with the privacy notices provided at or before collection, including the Privacy Notice in SCA's Enrolment Form and the privacy information provided when SCA searches for or creates a Unique Student Identifier (USI).

2. Scope

This policy applies to personal information handled by SCA in connection with prospective, current and former students, parents or guardians where relevant, employees, contractors, authorised representatives, workplace or placement contacts and other people who interact with SCA.

The policy applies to information held in electronic and hard-copy systems and to information handled by third parties acting on SCA's behalf.

3. Legislative and Regulatory Framework

SCA manages personal information having regard to the following requirements, as applicable:

- Privacy Act 1988 (Cth), including the Australian Privacy Principles (APPs) and the Notifiable Data Breaches (NDB) scheme
- Privacy and Other Legislation Amendment Act 2024, including APP 11.3 technical and organisational security measures applying from 11 December 2024, and automated decision-making transparency requirements commencing 10 December 2026
- National Vocational Education and Training Regulator Act 2011
- Standards for Registered Training Organisations 2025, including the Outcome Standards and Compliance Standards
- National Vocational Education and Training Regulator (Data Provision Requirements) Instrument 2020, as amended, including the 2026 data-streamlining amendments
- VET Information Standard and applicable national VET data reporting requirements
- Student Identifiers Act 2014 and Student Identifiers Regulation 2014
- applicable Commonwealth, state and territory legal, funding and contractual requirements.

4. Definitions

Personal information: information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether or not the information is true or recorded in a material form

Sensitive information: a category of personal information that includes, among other things, information about racial or ethnic origin, political opinions or associations, religious or philosophical beliefs, membership of professional or trade associations or trade unions, sexual orientation or practices, criminal records, health or genetic information, and specified biometric information

APPs: the Australian Privacy Principles in Schedule 1 of the Privacy Act 1988

USI: Unique Student Identifier

NCVER: National Centre for Vocational Education Research

5. Privacy Governance and Collection Notices

SCA takes reasonable steps to implement practices, procedures and systems that support compliance with the APPs and allow privacy enquiries and complaints to be handled appropriately. This includes staff awareness and training, access controls, review of information-handling practices, management of service providers and review of privacy risks when systems or processes change.

Where required, SCA provides a collection notice at or before the time personal information is collected. The Enrolment Form includes the current VET Privacy Notice explaining the national VET reporting disclosures and the consequences that may arise if required information is not provided. A separate USI privacy notice or authorisation is provided where SCA searches for or creates a USI on a student's behalf.

6. Personal Information SCA Collects and Holds

Depending on the person and the service being provided, SCA may collect and hold the following kinds of information:

- identity and contact details, including name, date of birth, address, telephone number and email address
- emergency contact and, where a student is under 18, parent or guardian details
- USI information and identification documents where specifically required for USI creation, funding eligibility, licensing or course entry requirements
- employment information, employer or sponsor details and employment status
- education history, previous qualifications, credit transfer and Recognition of Prior Learning evidence
- language, cultural and demographic information required or requested for VET reporting, including Aboriginal and/or Torres Strait Islander status and gender information
- disability, health, accessibility, learner support and reasonable adjustment information where relevant
- course, enrolment, funding, attendance, participation, training, assessment, results and certification records
- assessment evidence, including written work, workplace evidence and, where required, photographs, audio or video recordings
- work placement or workplace training information, including supervisor or host-employer information
- fees, payment arrangements and transaction records
- complaints, appeals, feedback, misconduct and incident records
- survey preferences and correspondence with SCA
- for employees and contractors, information reasonably required for recruitment, engagement, qualifications, payroll, performance, work health and safety and compliance purposes.

SCA seeks to collect only information that is reasonably necessary for its functions and obligations. Sensitive information is collected only where reasonably necessary and with consent, or where collection is otherwise permitted or required by law.

7. How SCA Collects Personal Information

SCA usually collects personal information directly from the individual, including through enrolment and other forms, email, telephone, the SCA website, student management or learning systems, training and assessment activities, work placement arrangements and direct interactions with staff.

Where reasonably necessary or authorised, SCA may also collect information from other sources, including employers or sponsors, workplace supervisors, funding bodies, government agencies, the USI Registry, previous education providers for verification purposes, authorised representatives and service providers acting on SCA's behalf.

If SCA receives unsolicited personal information, it will consider whether the information could have been collected under the APPs. If not, and if SCA is not otherwise legally required to retain it, SCA will take reasonable steps to destroy or de-identify it.

8. Why SCA Collects, Holds, Uses and Discloses Personal Information

SCA may collect, hold, use and disclose personal information for purposes that include:

- responding to enquiries and assessing applications, entry requirements, course suitability and eligibility
- processing and managing enrolments
- identifying learner support, LLND, accessibility and reasonable adjustment needs
- delivering, administering and assessing VET courses and other training services
- managing work placement or workplace training
- recording outcomes and issuing AQF certification documentation
- verifying, searching for or creating a USI where authorised
- determining and administering funding eligibility, subsidies, concessions and contractual requirements
- meeting national and state or territory VET data reporting requirements
- communicating with students, employers, sponsors and authorised representatives
- managing fees, payment arrangements and accounts
- supporting safety, wellbeing and emergency responses
- handling feedback, complaints, appeals, incidents and misconduct matters
- quality assurance, audit, regulatory reporting, continuous improvement and lawful business administration
- conducting or facilitating authorised student surveys and research

If information needed for enrolment, VET reporting, a USI, funding eligibility, certification, course entry or another legal requirement is not provided, SCA may be unable to enrol the person, report the training, verify or create a USI, determine eligibility, provide particular support or issue certification, as applicable.

9. VET Data Reporting and Government Disclosures

As an RTO, SCA is required to collect and report VET information. Personal information that forms part of reportable VET data may be provided directly to NCVER or to a state or territory training authority for onward reporting, in accordance with the National Vocational Education and Training Regulator Act 2011 and the Data Provision Requirements.

NCVER and relevant government bodies may use and disclose VET information for administration, regulation, monitoring, authenticated VET transcripts, statistics, research, surveys, data linkage, policy and workforce planning and other purposes authorised by law. Information may also be accessed by contracted IT operators supporting government VET data systems, subject to applicable privacy, security and confidentiality obligations.

The detailed, current VET disclosure wording is set out in the Privacy Notice included in SCA's Enrolment Form. Where the Privacy Notice is updated by law or the national VET data framework, SCA will update its collection notice accordingly.

Students may receive a survey from a government department, NCVER, an authorised agency, or a contractor acting for one of those bodies. Students may opt out of a survey at the time they are contacted, where the survey arrangements permit.

10. USI and Identification Documents

SCA verifies a student's USI before using it for VET purposes and obtains the required authorisation before searching for or creating a USI on a student's behalf. SCA provides the relevant USI privacy information when this occurs.

Identification documents are only requested where specifically required for USI creation, funding

eligibility, licensing or course entry requirements. Identification obtained solely for USI creation will not be retained unless another law or contractual requirement separately requires retention. SCA takes reasonable steps to protect USIs and related documentation from unauthorised access, use or disclosure.

11. Disclosure to Other Parties

SCA may disclose personal information where reasonably necessary for the purposes described in this policy, including to:

- ASQA, NCVER, DEWR, the Student Identifiers Registrar, state and territory training authorities, funding bodies and other government agencies or regulators where authorised or required
- service providers acting for SCA, such as student management, learning management, IT, cloud, communications, records, payment or student-support providers, where access is necessary to provide the service
- employers, sponsors, workplace supervisors or placement hosts where the disclosure is authorised, necessary for the training arrangement, or required by contract or law
- an authorised representative where the individual has provided authority
- health or emergency services where reasonably necessary to respond to a serious health or safety situation
- courts, tribunals, law enforcement bodies or other persons where disclosure is required or authorised by law.

SCA does not sell personal information. Where SCA engages a service provider, it takes reasonable steps appropriate to the arrangement to manage privacy and security risks and limit access to what is required for the service.

12. Overseas Disclosure

At the date of this policy, SCA is not currently likely to disclose personal information to overseas recipients as part of its ordinary RTO operations. If SCA proposes an arrangement that makes an overseas disclosure likely, SCA will consider the requirements of APP 8, take reasonable steps as required by law, and update this policy to identify the countries in which recipients are likely to be located where it is practicable to do so.

This section should be reviewed whenever SCA introduces or materially changes a cloud, software, support or service-provider arrangement that may involve access to personal information from outside Australia.

13. Automated Decision-Making

From 10 December 2026, APP 1 requires additional privacy-policy transparency where an organisation arranges for a computer program to make, or do something substantially and directly related to making, a decision that could reasonably be expected to significantly affect an individual's rights or interests, and personal information is used in the program.

Current position: SCA does not currently arrange for computer programs to make, or substantially and directly support, decisions of that kind using personal information. SCA will review this position when systems or processes change. If such automated decision-making is introduced, this policy will be updated to describe the kinds of personal information used and the kinds of decisions involved, as required by APP 1.7-1.9.

14. Data Quality, Security and Storage

SCA takes reasonable steps to ensure personal information it uses or discloses is accurate, up to

date, complete and relevant. Students and other individuals should tell SCA promptly if their name, address, email, phone number or other relevant information changes.

SCA takes reasonable technical and organisational measures to protect personal information from misuse, interference and loss and from unauthorised access, modification or disclosure. Measures may include, as appropriate:

- role-based and need-to-know access controls
- secure authentication, password and account-management practices
- secure systems, backups and appropriate protective technology
- locked or controlled storage for paper records
- staff confidentiality, privacy and information-security requirements and training
- reasonable due diligence and contractual controls for third-party providers
- incident and data-breach response processes

Security arrangements are reviewed having regard to the sensitivity and volume of information, changes in technology and the risks associated with SCA's systems and service-provider arrangements.

15. Retention, Destruction and De-identification

SCA retains student, training, assessment and certification records for the periods required by the VET regulatory framework, other laws, licensing requirements and applicable funding or contractual arrangements.

Under the 2025 RTO compliance requirements, SCA retains records of AQF certification documentation issued to VET students for 30 years and retains records of assessments submitted by a VET student for at least two years after the student completes the training product, unless a longer period applies under another requirement.

Identification obtained solely for USI creation is handled as described in section 10 of this policy. Other personal information is retained in accordance with SCA's Records Management Policy and applicable requirements.

When personal information is no longer required for a lawful purpose and SCA is not required by law or a court or tribunal order to retain it, SCA will take reasonable steps, including appropriate technical and organisational measures, to destroy the information or ensure it is de-identified.

16. Access and Correction

Individuals may request access to personal information SCA holds about them and may request correction if they believe the information is inaccurate, out of date, incomplete, irrelevant or misleading.

Requests may be made to the Compliance Manager (privacy contact) using the contact details in section 20. SCA may take reasonable steps to verify identity before providing access or making a correction.

SCA will respond within a reasonable period and will generally aim to finalise access and correction requests within 30 calendar days. There is no fee for making an access request or for requesting or making a correction. If permitted by law, SCA may charge a reasonable amount for the cost of providing access, and will advise the individual before doing so.

If SCA refuses access or correction in circumstances permitted by law, it will provide written reasons where required and information about available complaint options. Where required, SCA will take reasonable steps to associate a statement with information that is not corrected and to notify relevant third parties of a correction.

17. Direct Marketing

SCA does not use or disclose personal information for direct marketing unless permitted by the Privacy Act and other applicable law. Where consent is relied upon, SCA will obtain the appropriate

consent. Individuals may ask SCA to stop direct marketing at any time by using an unsubscribe option or contacting SCA.

18. Data Breaches

SCA maintains processes for responding to actual or suspected data breaches. A data breach may involve loss of personal information or unauthorised access to or disclosure of personal information.

SCA will take reasonable steps to contain and investigate a suspected breach, assess the risk of harm, take remedial action where possible and document the response. Where the NDB scheme applies, SCA will assess a suspected eligible data breach within the period required by law (generally within 30 days) and, if an eligible data breach has occurred, notify affected individuals and the Office of the Australian Information Commissioner (OAIC) as soon as practicable, unless an exception applies.

Suspected privacy or data-security incidents should be reported promptly to the Compliance Manager.

19. Privacy Complaints

A person who believes SCA has mishandled their personal information or breached the APPs may make a privacy complaint to the Compliance Manager using the contact details in section 20. A complaint should describe the issue and, where possible, the outcome sought.

SCA will handle privacy complaints objectively, confidentially and with procedural fairness. SCA will acknowledge the complaint as soon as practicable and will generally aim to provide an outcome within 30 calendar days. If more time is reasonably required, SCA will explain the reason and keep the complainant informed of progress.

If the person is not satisfied after giving SCA a reasonable opportunity to respond, they may contact the Office of the Australian Information Commissioner at www.oaic.gov.au. A privacy complaint that also concerns training, assessment or another SCA service may also be considered under SCA's Complaints and Appeals processes where relevant.

20. Anonymity and Pseudonymity

Where practicable and lawful, individuals may make general enquiries or provide general feedback without identifying themselves or by using a pseudonym. SCA cannot offer anonymity where identity is required to enrol a student, verify or create a USI, administer funding, conduct assessment, issue certification, meet VET reporting obligations, manage safety, or comply with another legal or contractual requirement.

21. Contact Details and Policy Availability

Privacy enquiries, access or correction requests, and privacy complaints may be directed to:

Compliance Manager

Star College Australia Pty. Ltd. - RTO 41267

Head Office: 18 Rawlins Street, Southport QLD 4215

Postal: PO Box 457, Nerang QLD 4211

Phone: 1300 206 000

Email: admin@sca.edu.au

Website: www.sca.edu.au

SCA makes this Privacy Policy available free of charge on its website and on request. If a person reasonably requires the policy in another accessible form, SCA will take reasonable steps to provide it in that form.

22. Policy Review

This policy will be reviewed at least annually and earlier where there is a significant change to privacy law, VET data requirements, SCA systems, service providers or information-handling practices. SCA will also review the automated decision-making statement whenever relevant systems or decision processes change.

23. Associated Documents

- SCA Enrolment Form and VET Privacy Notice
- SCA Student Handbook
- Records Management Policy
- Complaints Policy and Appeals Policy
- Data Breach Response Register and related incident-response procedures
- Staff confidentiality obligations and employment or contractor agreements
- USI privacy information and authorisation records
- applicable funding-program privacy notices and contractual requirements