LEVERAGE
ACADEMY
RTO 41017

Data Management and Privacy Policy and Procedures

Version 5.2 – August 2026

Version Control

Item	Summary of update	Version	Review date
1	New comprehensive Policy and Procedures document created to replace old, outdated policy suite.	2.0	09/08/2025
2	Further review for compliance with 2025 RTO Standards as part of continuous improvement. Combined the Privacy Policy and Data and Record Management Policy to create new Data Management and Privacy Policy.	3.0	11/02/2026
3	Deletion of repetitive phrases leftover from the combining together of the Data and Record Management Policy and Privacy Policy. Correction to some minor linguistic errors.	4.0	26/02/2026
4	Added Privacy Collection Notice to Appendix to ensure consistency in the wording across various documents. Added third party payment disclosure information.	5.0	01/04/2026
5	Added explicit reference to Hubspot, RTOSafe, aXcelerate, and Microsoft Sharepoint to policy and privacy collection notice.	5.1	29/04/2026
6	Clarified procedure for when a Learner requests the deletion of their personal information.	5.2	07/08/2026

Quality area	Student Support; Governance; Product Integrity; Accountability
2025 RTO Standards Alignment	Outcome Standards 2.1, 2.7, 2.8, 4.1 Compliance Standards 10, 20
Author	Leverage Academy
Status	Approved
Approved by	Bailey Compton
Approval Date	07/08/2026

Purpose

This policy outlines Leverage Academy (the Academy)'s commitment to protecting the privacy and confidentiality of learner, team members and stakeholder information and to outline the principles and procedures for managing learner data and records for the Academy. This policy ensures that all records, including learner information, assessment results, and administrative data, are securely stored, accurately maintained, and disposed of in alignment with the 2025 RTO Standards and relevant privacy legislation, including the Australian Privacy Principles (APP/s).

Scope

This policy applies to all personal and sensitive information collected, stored, and managed by the Academy, including information related to learners, Academy team members, and other stakeholders (current and past). This policy is to be read in conjunction with other legislative, regulatory, and internal policies and procedures that are deemed relevant.

This policy applies to all Academy team members involved in the creation, storage, management, and disposal of records within the Academy. The Academy is required to manage different types of records across its RTO operations, including but not limited to:

- **Learner Records:** Enrolment forms, identification documents, attendance records, assessment results, feedback, progress reports, CVs and resumes, payment records and course completion records.
- **Assessment Records:** Evidence of assessments, including completed assessment tasks, observation checklists, assessor feedback, videos and photographic evidence, portfolios, third-party reports and references and validation documentation.
- **Administrative Records:** Financial records, employee records, training and assessment strategies, policies, procedures, and compliance documentation.

Responsibilities

All Academy team members are responsible for upholding the privacy of its learners, with the CEO / Academy Manager holding overall responsibility for privacy compliance, including reporting to any regulating body.

Policy

Data Management and Privacy Principles

The Academy collects personal information for business operations and legal obligations.

The Academy ensures each individual:

- Knows why their information is being collected, how it will be used and who it will be disclosed to.
- Is made aware of any legal requirement for the Academy to collect the information.
- Is made aware of any consequences for not providing the information requested.
- Is able to access their personal information upon request.
- Does not receive unwanted direct marketing.

- Can ask for personal information that is incorrect to be corrected.
- Can make a complaint about the Academy if they consider that their personal information has been mishandled or misused in some way.
- Whether the information is likely to be disclosed to overseas recipients, and if so, which countries such recipients are likely to be located in.

Learners are made aware that if adequate information is not provided as requested, the Academy may not be able to process an application for enrolment to a nationally recognised training course.

The Academy will:

- Maintain accurate, complete, and reliable records of its operations, including training delivery, assessment processes, learner support services, and administrative processes;
- Ensure records are accurate, complete, and reliable, reflecting the true nature of transactions, assessments, and other activities;
- Ensure that its records are created, maintained, and disposed of in accordance with the relevant legal, regulatory, and accreditation requirements;
- Provide training and support to its Academy team members to ensure that they understand the importance of records management and are equipped with the necessary knowledge and skills to create, maintain, and dispose of records effectively;
- Ensure the record management system is secure, reliable, and accessible to authorised team members as needed;
- Regularly review and updates records management policies and procedures to ensure that they are aligned with best practices and the changing regulatory and accreditation requirements;
- Ensure that records are stored in a manner that preserves their integrity, confidentiality, and accessibility, and that they can be retrieved and accessed easily and quickly when required;
- Maintain records of certification for a period of **30 years** in accordance with the relevant regulatory and accreditation requirements; and
- Ensure that records are disposed of in a timely and secure manner in accordance with the relevant retention and disposal schedules.

Sensitive Information

Sensitive information is only collected by the Academy if a permitted general or health situation applies in accordance with the Privacy Act 1988 (Cth) (16A, 16B) such as:

- If the collection of the information is required or authorised by, or under, an Australian law or a court/tribunal order;
- If it is unreasonable or impracticable to obtain the individual's consent to the collection, use or disclosure; and
- If it is genuinely and reasonably believed that:
    - The collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of an individual, or to public health or safety.
    - Unlawful activity, or misconduct of a serious nature, that relates to the Academy's functions or activities has been, is being or may be engaged in, and the collection, use or disclosure is necessary in order for the entity to take appropriate action in relation to the matter.

- The collection, use or disclosure is reasonably necessary to assist any APP entity, body or person to locate a person who has been reported as missing.
- The collection, use or disclosure is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim.

Privacy risks and breaches are considered as part of the Academy's overall compliance and risk framework and are reported and escalated consistent with governance arrangements under the RTO 2025 Standards.

Procedures

Collection of Information – Privacy Notices

As a registered training organisation (RTO), the Academy collects a learner's personal information so the Academy can process and manage the enrolment in a vocational education and training (VET) course with the Academy. The Academy uses a learner's personal information to enable the RTO to deliver VET courses to learners, and otherwise, as needed, to comply with its obligations as an RTO.

Under the *Data Provision Requirements 2020*, the Academy is required to collect personal information about each learner and disclose that personal information to the National Centre for Vocational Education Research Ltd (NCVER).

Information is gathered through enrolment forms, training records, and online submissions. Personal details collected include contact info, employment and academic history, statistical background data, training records, and fees-related info.

The Academy's management team will ensure privacy notices are added to relevant forms and information such as but not limited to Enrolment Forms, website content and promotional materials (**see Appendix One**).

Storage and Use of Information

The Academy secures personal records both physically and electronically. Information is used for learner administration, training, issuing qualifications, and marketing training products offered by the Academy, if permitted. Individuals may opt out of marketing, and no information is shared with third-party marketers without consent.

Electronic Records Management

The Academy has implemented specialist systems to ensure ongoing compliance, including:

- **Secure Systems:** Electronic records will be stored in secure, password-protected systems with appropriate encryption and access controls. The Academy will use reliable software systems, including aXcelerate SMS and LMS (learning management system), Hubspot, RTOSafe, and Microsoft Sharepoint to manage electronic records.
- **Access Permissions:** Access to electronic records will be restricted based on job roles and responsibilities. Only authorised Academy team members will have access to specific records to ensure data security and privacy.

- **Data Backups:** Regular data backups will be conducted to ensure that records are protected against data loss due to technical failures, cyber-attacks, or other incidents. Backups will be stored securely offsite or in cloud-based storage with appropriate security measures.

Physical Records Management

Where the Academy holds physical records, the Academy understands the obligations of RTOs in relation to the storage and access of physical records, including:

- **Secure Storage:** Hard copy records will be stored in locked cabinets or secure rooms with access restricted to authorised personnel. Records must be kept in a controlled environment to prevent damage, theft, or loss.
- **Access Logs:** Access to physical records will be monitored and logged to ensure accountability and prevent unauthorised access.

Disclosure of Information

Personal information may be shared with (but not limited to) government bodies such as ASQA, NCVER, and the USI Registrar as required. Disclosure is only made with consent, legal requirements, or if it is necessary for public safety. Any disclosed party is restricted to using information solely for the purpose provided. Permissions are generally part of the enrolment process and documentation.

Personal information – including personal information contained on a learner's file – may be used, or disclosed by the Academy for statistical, administrative, regulatory and research purposes. The Academy may disclose a learner's information for these purposes to:

- Commonwealth and State or Territory government departments and authorised agencies; and
- NCVER.

Personal information that has been disclosed to NCVER may be used or disclosed by NCVER for the following purposes:

- Pre-populating RTO learner enrolment forms;
- Understanding how the VET market operates, for policy, workforce planning and consumer information;
- Administering VET, including program administration, regulation, monitoring and evaluation;
- Facilitating statistics and research relating to education, including surveys and data linkage; and
- Populating authenticated VET transcripts.

Learners may receive a survey which may be administered by a government department or NCVER employee, agent or third-party contractor or other authorised agencies. Please note, learners may opt out of the survey at the time of being contacted.

NCVER will collect, hold, use, and disclose personal information in accordance with the *Privacy Act*, the *National VET Data Policy* and all NCVER policies and protocols (including those published on NCVER's website at www.ncver.edu.au).

The NCVER may also disclose personal information to persons engaged by NCVER to conduct research on

NCVER's behalf. The NCVER does not intend to disclose a learner's personal information to any overseas recipients.

For more information about how the NCVER handles personal information please refer to the NCVER's *Privacy Policy* at www.ncver.edu.au/privacy

The Department of Employment and Workplace Relations (DEWR) is authorised by law, including the Privacy Act and the NVETR Act, to collect, use and disclose personal information to fulfil specified functions and activities.

For more information about how the DEWR handles personal information, please refer to the VET Privacy Notice at https://www.dewr.gov.au/national-vet-data/vet-privacy-notice

The Academy retains evidence that learners have acknowledged the following Privacy Notice and Learner Declaration as part of the enrolment process: https://www.education.gov.au/privacy-notice-and-learner-declaration

The Academy gives an undertaking that it will not, under any circumstances distribute, sell or disclose any private and confidential details to any party or third parties for the purpose of soliciting marketing materials.

Leverage Academy shares personal information securely with Leverage Solicitors and Leverage Listings, the two other companies that form Leverage Group, to create a seamless customer experience between the various services that Leverage Group offers. The Academy has taken all reasonable steps to ensure that Leverage Solicitors and Leverage Listings comply with APP 8.

Surveys

Learners may also receive a survey run by a government department or an NCVER employee, agent, third-party contractor or another authorised agency. Learners can opt out of the survey at the time of being contacted.

Payments, Payment Plans and Third-Party Providers

We use third-party payment providers, including Stripe and Afterpay, to process payments and offer payment plans for our courses and services.

When you make a payment or apply for a payment plan, you may be redirected to, or interact directly with, these third-party platforms. To facilitate payment processing, we may share limited personal information such as your name, contact details, and transaction information.

Payment plan approval is determined by the relevant third-party provider. Your enrolment, access to training, or continuation in a course may be conditional on successful payment or approval of a payment plan. If a payment is declined, cancelled, or not maintained, we may suspend or cancel your enrolment in accordance with our *Fees, Charges, and Refund Policy and Procedures*.

We do not collect or store your full payment card details. Payment information is handled securely by our payment providers in accordance with their own privacy policies.

We recommend that you review the privacy policies of these providers to understand how your personal information is collected, used, and disclosed:

- Stripe: https://stripe.com/privacy
- Afterpay: https://www.afterpay.com/en-AU/privacy-policy

These third-party providers may store or process your personal information outside of Australia. By using our services and proceeding with payment, you acknowledge and consent to this disclosure.

We take reasonable steps to ensure that any third-party service providers we engage handle personal information in a manner consistent with Australian privacy law.

Maintenance and Updating of Records

The Academy will manage and update records in accordance with this policy and regulatory requirements to ensure:

- **Accuracy and Timeliness:** All records must be kept up-to-date and accurately reflect the latest information. Academy team member responsible for record maintenance must ensure that data is promptly updated following assessments, enrolments, or changes in learner status.
- **Audit and Review:**
  - Regular audits of records will be conducted to verify their accuracy, completeness, and compliance with retention requirements.
  - All document authors or reviewers must follow a consistent approach to the development of documents, and follow all guidelines as set out in the below procedures. Document authors or developers must also ensure that prior to the development or revision of any document, approval to commence revision or development is granted by the CEO, RTO Training Manager or Compliance and Operations Manager (or their delegate).
  - Policies and procedures will be reviewed at least annually to ensure they are up to date, accurate and compliant. Other documents will be reviewed during continuous improvement processes. The compliance manager is responsible for ensuring that policies and procedures are reviewed by their due date.
  - Electronic files will be saved in the drafts folder on the company server until approved. Access to this folder may be restricted to Academy team members involved in document development and review.
  - Files are archived as they are superseded by a new version.
  - Files will not be deleted other than by an authorised person for maintenance purposes and only where a backup of the data exists.

- **Document approval:**
  - All documents are subject to approval prior to use by any Academy team member. Approval must be given for every document by the authorised person specified within the below procedure.
  - Approved documents will be moved from the drafts folder and saved centrally for access by Academy team member on the company document server.

USI Authority and Identification documents

All participants (excluding overseas-based learners) will be required to provide a Unique Student Identifier (USI) under the *Learner Identifiers Act 2014*. A clear statement that USIs will only be used for purposes permitted under the Student Identifiers Act 2014 and associated rules and will not be published or used as a general student number.

Each learner's USI provides access to a secure online account that contains all their training records and results completed since the commencement of the USI on 1 January 2015, a Commonwealth government requirement. The Academy can obtain consent from the participant to search or verify a USI on their behalf.

USIs are collected by the Student Liaison team via a completed *Enrolment Form* submitted by each learner.

All learners (excluding overseas-based learners) must be able to provide a USI before a Registered Training Organisation (RTO) such as Leverage Academy can issue a Qualification Certificate, Record of Results and / or Statement of Attainment (SOA) upon successful completion of units of competency.

Where a learner does not have a USI, they can create one at https://www.usi.gov.au/students/create-\r-usi where the learner will need to provide their personal information, contact information and suitable identification.

USI Portal and AVETMISS Data Collection

The Academy has implemented additional measures to ensure compliance and the mitigation of human error when updating the USI Portal via the aXcelerate SMS and the AVETMISS Data Collection platform.

All Academy team members uploading course information for new or superseded qualifications or individual units on the Academy's scope of registration must follow each step on the *SI Portal Flowchart* to ensure the following:

- The Packaging Rules for the qualification have been correctly applied, taking priority over any unit(s) that may have been superseded prior to qualification's delivery period ending;
- All information – including qualification / unit code and title as well as course parameters – is checked and any errors are corrected in aXcelerate before the AVETMISS platform is updated;
- Academy team members must not override any information in relation to qualification / unit code and title, and course parameters. If, in the event, incorrect information must be overridden, the Academy team member must check with the Academy's Operations and Compliance Manager prior to overriding the system.
- Any updates to aXcelerate must also be transferred to AVETMISS to ensure the changes are reflected across aXcelerate, AVETMISS and the USI Portal. Incorrect information could, in the most extreme circumstances, lead to qualifications / statements of attainment being deemed null and void and consequently on flowing licensing application and / or cancellation issues.

Note – AVETMISS automatically uploads to the USI Portal used to update a learner's USI Transcript.

Please refer to the *Learner Handbook* for detailed instructions on the generation of USIs.

Request to Access records

Individuals may request to access their records by completing the *Access to Records Request Form* and submitting it via email to info@leverageacademy.edu.au. All requests for access to personal information and records must be made in writing as the individual must be able to identify themselves and verify their identity prior to any information being disclosed.

Requests can be submitted from past or current learners or other individuals to access records held in a file about a learner, or access to a previously issued AQF certification document. Please refer to this policy the and the *AQF Certification Policy and Procedures* for more information.

Upon receiving a completed form, the Academy's Student Liaison team will:

- Confirm the request is valid and has been made by the individual to which the records relate (i.e. check identification documents);
- Make arrangements for the provision of accessed records (i.e. mailing copies, providing a time for records to be viewed etc.).
- Confirm arrangements in writing within 14 days of receiving the request.
- Mail records, where requested, to the address that is held on file for that individual, unless an alternate address is provided along with proof of identity (e.g. a driver's license or utility bill).
- Ensure the learner has provided photo ID prior to being shown records in person. The ID should be matched to records held on file for the individual to confirm they are only viewing their own records.
- Make a note on how the records were accessed on the individual's secure file and record information in the aXcelerate SMS if applicable.

There is no charge to access learner records however there is a cost of 50c per page for photocopying or printing.

Request for Amendments to Records

Past learners who have received issued qualifications, records of results and / or statements of attainment (SOAs) from the Academy can request for incorrect records held about them to be corrected. To have records and details amended, including certificate reprint, learners must make their request in writing by completing the *Amendment to Records Request Form* and submitting it via email to info@leveragegroup.com.au.

Upon receipt of a completed request form, the Academy's Student Liaison team will consider whether the records held are correct or not. If the request is valid and records are incorrect, the Academy will update the records accordingly. Records will not be updated if they are found to be correct.

If a request has been received to re-issue a qualification in a name that has been changed legally, a processing fee of $75 must be paid prior to the Academy generating the re-issued qualification.

Current learners who wish to update their personal information must complete the *Change of Details Form* and submit it via email to info@leveragegroup.com.au.

The Academy will advise the individual in writing within 14 days of the actions taken to amend their records.

Retention and Disposal of Records

The Academy will abide by all regulatory requirements and implement best practice approaches to the retention and disposal of records.

Retention Periods

- **Learner Records:** Learner records, records of all AQF certification documentation issued, including assessment results and course completion records, will be retained for a minimum of **30 years** as required by regulatory standards.
- **Learner Assessment Records:** Learner assessment records, including but not limited to assessment workbooks, practical skills assessment evidence will be retained for a minimum of **two (2) years** as required by regulatory standards.
- **Financial and Administrative Records:** These records will be retained for a minimum period specified by relevant legislation, typically **seven (7) years**.

Secure Disposal

- **Electronic Records:** Electronic records will be securely deleted from all systems, ensuring that data cannot be recovered or reconstructed.

Hard Copy Records: Physical records will be disposed of through secure shredding or incineration to prevent unauthorised access to sensitive information. This may be conducted via external professional services.

Disposal Request from Learner

A learner may request for the disposal and deletion of any personal information held by the Academy. The following process applies:

1. Confirm the Learner's identity either face-to-face, or via video call with reference to an official Government-issued ID (e.g., driver's licence).
2. Explain the consequences of deleting the Learner's information, such as that they will no longer be able to access the Academy's services, and that certificates cannot be reissued.
3. Request the request be put in writing (such as via email) stating that the Learner understands and accepts the consequences for deletion of their personal information.
4. Delete the Learner's records across the platforms in which it is stored.
5. Confirm in writing to the Learner once these actions have been completed.
6. Log an internal note within aXcelerate detailing the reason for the removal of the student data with the attached written request and acknowledgement from the student.

Note that we can only delete the personal information that we hold; for example, the Academy cannot delete a Learner's USI number – that is handled by the relevant authority if they no longer wish to have a USI number.

Complaints

Complaints regarding information handling will be addressed by the Academy in accordance with the Academy's *Complaints and Appeals Policy and Procedures*. Outcomes of complaints and any related appeals may be used as inputs to continuous improvement.

If a learner has concerns about how the Academy is managing personal information, they are encouraged to inform Academy team members of the Academy and discuss their concern. Learners can also make a complaint directly to the Academy using the *Complaint Form* and submitting it via email to info@leverageacademy.edu.au.

Under the Privacy Act 1988 (Cth), learners also have the right to make a complaint to the office of the Australian Information Commissioner (OAIC) about the handling of personal information. More information about making a privacy complaint can be found at: http://www.oaic.gov.au/privacy/privacy-complaints.

Data Breach Management

Incident Response
In the event of a data breach or suspected data security incident, the Academy will immediately assess the situation, contain the breach, and take action to prevent further unauthorised access.

Reporting and Notification
Significant data breaches will be reported to relevant authorities including the police, and affected individuals will be notified in accordance with the Privacy Act 1988 (Cth) and any other applicable legislation by the Responsible Person.

Where the data breach relates to sensitive information and poses serious harm to any stakeholder, the Academy will report the data breach to the Officer of the Australian Information Commissioner within **five (5)** business days.

Academy Team Member Training and Management

Academy team members who are involved in records management will receive regular training on data security, privacy, and compliance requirements to ensure they are aware of their responsibilities and the regulatory requirements of RTOs.

Academy team members handling sensitive records will be required to sign confidentiality and privacy agreements, acknowledging their commitment to protecting learner and organisational information.

Policy Governance

Review
All systems and materials in relation to privacy and data and record management systems must be reviewed and approved by the Academy Manager before publication to ensure compliance with RTO standards and regulatory requirements.

On-going Monitoring and Compliance

The Academy will regularly monitor its privacy-related processes and data and record management processes to ensure ongoing compliance and will promptly address any non-compliant practices or areas of improvement identified, and document this in the *Continuous Improvement Register* accordingly.

Definitions

- **ASQA** means Australian Skills Quality Authority, the national VET regulator and the RTO's registering body.
- **Australian Privacy Principles (APPs)** refers to the principles govern how entities handle personal information, including collection, use, disclosure, and storage.
- **APP Entities** collectively refers to the organizations and agencies covered by the APPs.
- **Compliance Standards** refers to the Compliance Standards for National Vocational Education and Training Regulator (NVR) Registered Training Organisations (RTOs) Instrument 2025.
- **Consent** means an individual's agreement to the collection, use, or disclosure of their personal information. This agreement can be either express (explicitly stated) or implied (inferred from conduct). For consent to be valid under the Privacy Act, it must be voluntary, informed, specific, current, and given by someone with the capacity to understand.
- **Data Security** refers to measures taken to protect electronic and physical records from unauthorized access, theft, alteration, loss, or destruction.
- **Learner Records** refers to documents and data related to learners, including (but not limited to) enrolment details, assessment results, attendance records, course progress, and other personal information.
- **Organisation** means any person, company, partnership, unincorporated group, or trust that is not a small business, political party, government agency, State or Territory authority, or a listed public body.
- **Outcome Standards** refers to the Outcome Standards for National Vocational Education and Training Regulator (NVR) Registered Training Organisations (RTOs) Instrument 2025.
- **Personal information** means information or an opinion about an identified individual, or an individual who is reasonably identifiable:
    - Whether the information or opinion is true or not; and
    - Whether the information or opinion is recorded in a material form or not.
- **Records Management** means the systematic control of records throughout their lifecycle, including (but not limited to) creation, maintenance, use, storage, and disposal, in a manner that supports operational and compliance requirements.
- **Retention Period** refers to the duration for which records must be kept in accordance with regulatory or legal requirements before they can be disposed of.
- **Responsible Person** means a person nominated by the individual to be contacted in case of emergency.
- **Sensitive Information** means details about (but not limited to) racial or ethnic origin, political opinions, religious beliefs, health information, and more.
- **Student Management System (SMS)** refers to a software solution designed to manage all aspects of student data and administrative processes within a training organisation. It streamlines operations, enhances efficiency, and helps RTOs meet compliance requirements.

- **Unique Student Identifier (USI)** is a unique reference number issued to an individual by the Australian Government, in accordance with the Student Identifiers Act 2014. It is made up of numbers and letters and enables an individual to look up and track their training achievements in an online database.

Appendix One: Privacy Collection Notice

Why Leverage Academy collects your personal information
As a registered training organisation (RTO), Leverage Academy (the Academy) collects a learner's personal information so the Academy can process and manage the enrolment in a vocational education and training (VET) course with the Academy.

If adequate information is not provided as requested, the Academy may not be able to process applications for enrolment in a nationally recognised training course. We do not collect or store your full payment card details. Payment information is handled securely by our payment providers in accordance with their own privacy policies.

How personal information is used
The Academy uses a learner's personal information to enable the RTO to deliver VET courses to learners and otherwise, as needed, to comply with its obligations as an RTO.

How personal information is disclosed
The Academy shares personal information securely with Leverage Solicitors and Leverage Listings, the two other companies that form Leverage Group, to create a seamless customer experience when you wish to access other services that Leverage Group offers.

The Academy is required by law – under the *National Vocational Education and Training Regulator Act 2011 (Cth)* (NVETR Act) – to disclose the personal information collected about a learner to the National VET Data Collection kept by the National Centre for Vocational Education Research Ltd (NCVER). The NCVER is responsible for collecting, managing, analysing and communicating research and statistics about the Australian VET sector.

The Academy is also authorised by law – under the NVETR Act – to disclose a learner's personal information to the relevant state or territory training authority.

We use third-party payment providers, including Stripe and Afterpay, to process payments and offer payment plans for our courses and services. When you make a payment or apply for a payment plan, you may be redirected to, or interact directly with, these third-party platforms. To facilitate payment processing, we may share limited personal information such as your name, contact details, and transaction information.

Payment plan approval is determined by the relevant third-party provider. Your enrolment, access to training, or continuation in a course may be conditional on successful payment or approval of a payment plan. If a payment is declined, cancelled, or not maintained, we may suspend or cancel your enrolment in accordance with our *Fees, Charges, and Refund Policy and Procedures*.

We store personal information in secure systems, namely Hubspot, aXcelerate, and Microsoft Sharepoint.

How the NCVER and other bodies handle learners' personal information
The NCVER will collect, hold, use and disclose learners' personal information in accordance with the law, including the *Privacy Act 1988 (Cth)* (Privacy Act) and the NVETR Act. A learner's personal information may be used and disclosed by NCVER for purposes that include populating authenticated VET transcripts;

administration of VET; facilitation of statistics and research relating to education, including surveys and data linkage; and understanding the VET market.

The NCVER is authorised to disclose information to the Australian Government Department of Employment and Workplace Relations (DEWR), Commonwealth authorities, State and Territory authorities (other than registered training organisations) that deal with matters relating to VET and VET regulators for the purposes of those bodies, including to enable:

- Administration of VET, including program administration, regulation, monitoring and evaluation
- Facilitation of statistics and research relating to education, including surveys and data linkage
- Understanding how the VET market operates, for policy, workforce planning and consumer information.

The NCVER may also disclose personal information to persons engaged by NCVER to conduct research on NCVER's behalf.

The NCVER does not intend to disclose a learner's personal information to any overseas recipients.

Stripe and Afterpay may store or process your personal information outside of Australia. By using our services and proceeding with payment, you acknowledge and consent to this disclosure.

We take reasonable steps to ensure that any third-party service providers we engage handle personal information in a manner consistent with the Australian Privacy Principles.

For more information about how the NCVER will handle your personal information please refer to the NCVER's Privacy Policy at www.ncver.edu.au/privacy.

For more information on how Stripe, Afterpay, RTOSafe, Hubspot, aXcelerate, and Microsoft Sharepoint handle your personal information please refer to their privacy policies available on their websites:

- Stripe: https://stripe.com/privacy
- Afterpay: https://www.afterpay.com/en-AU/privacy-policy
- Hubspot: https://legal.hubspot.com/privacy-policy
- AXcelerate: https://www.axcelerate.com.au/privacy-policy
- Microsoft Sharepoint: https://www.microsoft.com/en-gb/privacy/privacystatement
- RTOSafe: https://rtosafe.com.au/privacy-policy.pdf

If you would like to seek access to or correct any of your information, in the first instance, please contact the Academy.

DEWR is authorised by law, including the Privacy Act and the NVETR Act, to collect, use and disclose your personal information to fulfil specified functions and activities.

For more information about how the DEWR will handle your personal information, please refer to the DEWR VET Privacy Notice at https://www.dewr.gov.au/about-department/resources/dewr-privacy-policy

Surveys

You may receive a learner survey which may be run by a government department or an NCVER employee, agent, third-party contractor or another authorised agency. Please note you may opt out of the survey at the time of being contacted.

Contact information

At any time, you may contact Leverage Academy on **1300 438 538** or info@leverageacademy.com.au to:

- Request access to your personal information;
- Correct your personal information;
- Make a complaint about how your personal information has been handled; and / or
- Ask a question about this Privacy Notice

For information about how Leverage Academy collects, uses and discloses your personal information generally, including how you can make a complaint about a breach of privacy, please refer to the Academy's *Data Management and Privacy Policy and Procedures*.