

1. Introduction

Catapult Smallprint Pty Ltd are committed to protecting the privacy of the individuals whose personal information we collect, hold, use and disclose.

This Privacy Policy explains how we manage personal information when people use our websites, platforms, learning management systems, student management systems, online services, support channels, products, integrations and other services.

This Policy applies to personal information collected from or about customers, learners, students, administrators, trainers, assessors, website visitors, prospective customers, business contacts, suppliers, contractors and other individuals who interact with us.

Where we provide a platform or service on behalf of a customer, such as a registered training organisation, employer, school, education provider or other organisation, that customer may also have its own privacy policy and legal obligations. In those cases, we may process personal information on behalf of that customer as part of delivering the contracted service.

2. Definitions

In this Policy:

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 it is recorded in a material form or not.

Sensitive information is a category of personal information that may include information about health, racial or ethnic origin, political opinions, religious beliefs, trade union membership, criminal record, biometric information and other information treated as sensitive under applicable privacy laws.

We, us and our means AdNeo Pty Ltd and its related businesses, including Catapult and Vasto, unless the context requires otherwise.

Platform means the software, systems, websites, learning management systems, student management systems, integrations, support services and related services provided by us.

3. What personal information we collect

We collect the personal information reasonably necessary for our business activities, for providing our products and services, and for meeting legal, regulatory and contractual obligations.

The types of personal information we may collect include:

- name, business name, role, job title and organisation;

- contact details such as email address, phone number, postal address and billing address;
- account details, usernames, password-related authentication information and security settings;
- learner, student, enrolment, course, training, assessment and participation information;
- examination results, grades, records of competence, submissions, responses, messages, feedback and support interactions;
- information uploaded to or entered into our platforms by users or customers;
- payment, invoicing and transaction information, noting that full payment card details may be handled by third-party payment providers rather than stored directly by us;
- technical and usage information, including IP address, browser type, operating system, device information, referral source, log data, pages viewed, access times, activity logs and navigation behaviour;
- communications with us, including emails, support tickets, calls, chat messages, meeting notes and feedback;
- marketing preferences, event registrations and survey responses;
- information required to investigate security, support, compliance or contractual issues; and
- any other information that an individual or customer chooses to provide to us.

We may collect sensitive information where it is reasonably necessary for the services we provide, where the individual has consented, where the information has been provided to us by a customer for a permitted purpose, or where collection is otherwise permitted or required by law.

4. How we collect personal information

We may collect personal information:

- directly from an individual, including when they create an account, use a platform, complete a form, submit an assessment, contact support, make an enquiry, register for an event or communicate with us;
- from our customers, including training organisations, employers, education providers, administrators, trainers, assessors and other authorised users;
- from platform usage, system logs, cookies, analytics tools and security monitoring tools;
- from third-party systems or integrations authorised by a customer or user;
- from payment providers, identity providers, communication providers and other service providers;
- from publicly available sources; and
- from related bodies corporate or businesses within the AdNeo group.

Where a customer or user provides us with another individual's personal information, they must ensure they have the right to do so and that the individual has been given any required privacy notice or consent.

5. Why we collect, use and disclose personal information

We collect, use and disclose personal information for purposes connected with our business, products and services, including to:

- provide, operate, administer and support our platforms and services;
- create and manage user accounts;
- deliver learning management, student management, training, assessment and reporting functions;
- store, transmit and collate enrolments, submissions, grades, examination results, records of competence, messages and feedback;
- enable communications between administrators, trainers, assessors, students, learners, customers and other authorised users;
- provide customer support, technical support, billing support and service notifications;
- process payments, invoices, refunds and account administration;
- implement customer instructions, including configuration, migration, integration, reporting and data export requests;
- provide integrations with authorised third-party systems;
- improve, test, maintain and secure our products and services;
- monitor usage, performance, availability, errors, security events and compliance with platform terms;
- conduct analytics, reporting, research, product development and service improvement;
- communicate with customers and users about products, services, upgrades, updates, incidents, security matters and changes that may affect them;
- conduct surveys, training, events, webinars, promotional activities and marketing where permitted;
- meet legal, regulatory, contractual, audit, insurance and governance obligations;
- investigate or respond to complaints, disputes, suspected fraud, security incidents, data breaches or misuse of our services;
- protect our rights, property, systems, users and customers; and
- support a merger, acquisition, sale, restructure or transfer of all or part of our business or assets.

We will not sell personal information.

6. Direct marketing

We may use personal information to send information about our products, services, events, updates or other matters we believe may be relevant to customers or business contacts, where permitted by law.

Individuals may opt out of receiving marketing communications at any time by using the unsubscribe function in an electronic communication or by contacting us directly.

We will not disclose personal information to a third party for that third party's direct marketing purposes without consent.

7. Artificial intelligence and automated tools

We may use approved artificial intelligence, machine learning, automation, analytics or similar tools to support our business operations and services. This may include use for document drafting, summarisation, support workflows, product improvement, security monitoring, data analysis, knowledge management, content generation, assessment support, AI-detection or plagiarism-detection workflows, and other approved business purposes.

Where AI or automated tools process personal information, we will apply privacy, security and data minimisation controls appropriate to the use case. We will not intentionally submit personal information, confidential customer data or regulated data into unapproved AI tools.

AI tools are used to support human work and decision-making. We do not rely on AI systems to make final decisions about individuals where human review is required by law, contract or internal policy.

Where a customer enables or requests an AI-related feature, we may process the relevant information as reasonably necessary to provide that feature. Product-specific notices, customer agreements or platform terms may provide further details about particular AI features.

8. Disclosure of personal information

We may disclose personal information to:

- employees, contractors and authorised personnel who need access to perform their roles;
- related bodies corporate and businesses within the AdNeo group;
- customers and authorised users, including training organisations, administrators, trainers, assessors, employers, education providers and other account administrators;
- third-party providers of systems, hosting, cloud infrastructure, security, monitoring, email, messaging, payment processing, analytics, support, identity management, development, testing and other business services;
- integrators, student management systems, training management systems, learning tools and other third-party systems authorised by a customer or user;
- professional advisers, insurers, auditors, consultants and legal representatives;
- government agencies, regulators, courts, tribunals, law enforcement bodies or other parties where required or authorised by law;
- parties involved in an actual or proposed merger, acquisition, restructure, sale or transfer of our business or assets;
- any person or organisation authorised by the individual or customer; and
- any other person or organisation where disclosure is permitted or required by law.

We take reasonable steps to ensure that third-party service providers handle personal information consistently with applicable privacy and security obligations.

9. Cross-border disclosure and data residency

Some of our platforms and services are hosted in Australia. Some third-party service providers, support services, cloud services or integrations may store, process, access or support data from locations outside Australia.

Where we disclose personal information to an overseas recipient, we will take reasonable steps required by applicable privacy laws to ensure the recipient handles the information appropriately, unless an exception applies, such as where:

- the individual has consented;
- the disclosure is required or authorised by law;
- the recipient is subject to privacy protections substantially similar to the Australian Privacy Principles; or
- another exception under applicable privacy law applies.

Product-specific hosting, data residency or on-shoring commitments may be set out in customer agreements, product schedules, security statements or other written commitments. Where a customer agreement contains stricter data residency obligations, those obligations will apply to the relevant service.

10. Security of personal information

We take reasonable technical and organisational steps to protect personal information from misuse, interference, loss, unauthorised access, modification and disclosure.

These steps may include:

- access controls and role-based permissions;
- unique user accounts and authentication controls;
- multi-factor authentication for selected systems and privileged users;
- password and credential management controls;
- encryption of data in transit and, where appropriate, at rest;
- secure hosting and network protections;
- firewalls, monitoring, vulnerability management and logging;
- backup, disaster recovery and business continuity processes;
- staff training and confidentiality obligations;
- vendor security review processes;
- incident response and breach assessment processes; and

- internal policies covering data protection, acceptable use, access control, AI use, security incident response and related matters.

No method of transmission or storage is completely secure. While we take reasonable steps to protect personal information, we cannot guarantee the security of information transmitted over the internet or stored electronically.

Users are responsible for keeping their login details confidential and for complying with any account security requirements notified to them.

11. Data retention, deletion and de-identification

We retain personal information for as long as reasonably necessary for the purposes for which it was collected, including to provide our services, comply with legal and regulatory obligations, meet contractual requirements, resolve disputes, maintain business records, support security and audit requirements, and protect our legitimate interests.

Where we no longer need personal information for a permitted purpose, we will take reasonable steps to destroy or de-identify it, unless we are required or authorised to retain it by law, contract, audit requirement, dispute, investigation or other legitimate business need.

Where a customer controls the relevant account, course, enrolment, organisation or platform environment, requests for access, correction, deletion or export may need to be directed to that customer in the first instance. We may also assist customers to action requests where required under the relevant agreement or applicable law.

12. Accessing and correcting personal information

Individuals may request access to personal information we hold about them or ask us to correct information they believe is inaccurate, out of date, incomplete, irrelevant or misleading.

Requests should be made in writing using the contact details in this Policy. We may need to verify the identity of the person making the request before providing access or making a correction.

We will respond within a reasonable period. We may decline access or correction in circumstances permitted by law, including where providing access would have an unreasonable impact on the privacy of others, where the request is frivolous or vexatious, where access would be unlawful, or where we cannot verify the requester's identity.

We will not charge a fee for making an access or correction request. We may charge a reasonable fee for providing access where permitted by law and where the cost is not excessive.

13. Anonymity and pseudonymity

Where lawful and practicable, individuals may deal with us anonymously or using a pseudonym. However, this may limit our ability to provide services, respond to requests, verify identity, provide support, maintain accurate records or meet contractual, legal or regulatory obligations.

14. Cookies, analytics and website technologies

Our websites and platforms may use cookies, local storage, analytics tools and similar technologies to operate services, maintain sessions, improve usability, remember preferences, monitor performance, analyse usage, protect security and improve our products and services.

Cookies are small files or records stored by a browser or device. Some cookies are necessary for a website or platform to function. Others support analytics, preferences, security or marketing.

Users may be able to disable cookies through their browser settings. Disabling cookies may affect the functionality or usability of our websites and platforms.

15. Third-party websites and integrations

Our websites and platforms may contain links to third-party websites, applications, services or integrations. We are not responsible for the privacy practices, security controls or content of third-party websites or services, except to the extent required by law.

Users should review the privacy policies and terms of those third parties before using them or providing personal information.

16. Data breaches and security incidents

We maintain processes for assessing and responding to suspected privacy or security incidents.

If we become aware of unauthorised access, disclosure or loss of personal information, we will assess the incident and take reasonable steps to contain, investigate and remediate it.

Where required by law, including under the Notifiable Data Breaches scheme, we will notify affected individuals and the Office of the Australian Information Commissioner, or support the relevant customer to do so where the customer is responsible for notification.

17. Complaints and enquiries

Individuals may contact us if they have questions about this Policy, wish to access or correct personal information, wish to opt out of marketing, or believe we have not handled their personal information appropriately.

Privacy contact: **security@catapulteducation.com.au**

Postal address: **Building 5, 938 South Road, Edwardstown SA 5039**

We take privacy complaints seriously and will respond within a reasonable period. We may ask for further information to help us investigate and respond.

If an individual is not satisfied with our response, they may contact the Office of the Australian Information Commissioner at **www.oaic.gov.au**.

18. Changes to this Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our business, products, services, technology, legal obligations or privacy practices.

The current version will be made available on our website or otherwise provided on request. The effective date or last reviewed date will indicate when the Policy was last updated.