



APEX DATA SOLUTIONS

Privacy Policy

Apex Data Solutions Pty Ltd

FOR CUSTOMERS AND ASSESSORS

Document	Privacy Policy
Version	Version 1.7
Date	5 September 2026
Issued by	Apex Data Solutions Pty Ltd
Audience	Customers, prospective customers and assessors

Apex Data Solutions Pty Ltd | ABN 71 670 512 857 | 13 Draper Avenue, Roselands NSW 2196
www.apexdatasolutions.com.au | admin@apexdatasolutions.com.au

1. WHO WE ARE

Apex Data Solutions Pty Ltd (ABN 71 670 512 857) is an Australian company based in New South Wales. We operate the Apex Platform, a browser-based analytics tool used by school staff to analyse student assessment data, and we deliver Data Strategy Sessions, which are professional learning sessions for school staff.

This policy explains how we handle personal information.

Contact: admin@apexdatasolutions.com.au

2. THE PRIVACY LAWS WE COMPLY WITH

We have committed to handling personal information in accordance with the following, whether or not we are otherwise required to.

- The **Australian Privacy Principles** under the *Privacy Act 1988* (Cth). We have committed in our customer contracts to comply with the Australian Privacy Principles.
- The **Information Protection Principles** under the *Privacy and Personal Information Protection Act 1998* (NSW) and the **Health Privacy Principles** under the *Health Records and Information Privacy Act 2002* (NSW), when handling information on behalf of a NSW government school.
- The **Notifiable Data Breaches** scheme under Part IIIC of the *Privacy Act 1988* (Cth) and, where we act for a NSW agency, the **Mandatory Notification of Data Breach** scheme under Part 6A of the *Privacy and Personal Information Protection Act 1998* (NSW).

3. TWO CATEGORIES OF INFORMATION

We handle two categories of information, and they are subject to different rules. They are dealt with separately throughout this policy.

3.1 School Data

School Data is the student assessment and enrolment information a school uploads to the Apex Platform so that we can analyse it and produce reports for that school.

School Data is owned by the school. We hold it on the school's behalf and act on the school's instructions.

If you are a student, parent or carer and you want to know what information a school holds about you, or you want it corrected, that request goes to the school. We assist the school to respond.

School Data typically includes: student name, student identifier, year level, class and cohort, and NAPLAN and other assessment results.

What School Data must not include. Our contracts require schools not to upload health information, disability records, counselling or wellbeing notes, child protection records, behaviour or discipline narratives, or family, custody or court information. The Platform is not designed to hold this material.

3.2 Our own records

This is information about the adults we deal with: school staff who use the Platform, people who contact us, and staff at schools we approach about our services.

Information we hold about school staff outside the Platform for our own business purposes, being work contact details obtained from publicly available sources or given to us directly, correspondence, and records of our dealings with a school, is our own business record. It is not School Data, and it is not held on a school's behalf. It is still personal information, and we handle it under the Australian Privacy Principles as described in this policy.

3.3 Reports prepared outside the Platform

Apex has previously prepared analysis for schools manually and supplied it as PDF reports rather than through the Platform. Where Apex holds source data for that purpose, it is held in Microsoft OneDrive with Australian data residency, is used only to prepare reports for the school that supplied it, and is subject to the same restrictions set out in section 5 and the same retention position set out in section 10.

4. WHAT WE COLLECT AND WHY

The table below sets out every category of personal information we collect, why we collect it, and where it comes from.

Whose details	What we collect	Why	Source
Students	Name, student identifier, year level, class and cohort, assessment results	To produce the analysis and reports the school has asked us for	The school, by upload to the Platform. We do not collect it from students, and students cannot access the Platform.
School staff using the Platform	Name, work email address, school, role, login and activity records, and a mobile phone number provided voluntarily for two-factor authentication	To create and manage accounts, send two-factor authentication codes, provide support, maintain security, and investigate misuse	The school, or the staff member
People who contact us	Name, email, phone, school, and the content of the enquiry	To respond to the enquiry and keep a record of it	The person
School contacts we approach	Name, role, school, work email, work phone, and publicly available school information including enrolment and ICSEA	To inform schools about our services and to record who we have contacted	Publicly available sources, including the NSW Department of Education public schools dataset and school websites, and from people who provide their details
Session participants	Name, school, role, registration details	To organise and deliver a Data Strategy Session	The school or the participant

5. RESTRICTIONS ON OUR USE OF SCHOOL DATA

These restrictions are contractual. They appear in our Terms of Service as well as in this policy.

We do not sell, rent, licence or trade School Data.

We also do not:

- use School Data for advertising or marketing, or to market to students, parents or carers;
- use School Data to train artificial intelligence or machine learning models;
- use School Data to build a profile of an individual student for any purpose other than producing reports for that student's school;
- share School Data with any other school, or use one school's data to produce anything for another school;
- use School Data for benchmarking, research or product development, or to create aggregated or de-identified datasets for our own purposes; or
- transfer School Data outside Australia, or allow it to be accessed from outside Australia.

The Apex Platform does not use artificial intelligence. Its recommendations are produced by rules we have written, and any figure the Platform displays can be traced to the rule that generated it. If this changes, we will notify school customers at least 60 days in advance and they may terminate their subscription.

6. WHERE INFORMATION IS STORED

6.1 School Data and staff account information

Student data is stored in Australia. All student assessment and enrolment data uploaded to the Apex Platform is held on Microsoft Azure in Australian data centres. It is not transferred outside Australia and is not accessible from outside Australia, including by our own personnel.

Staff account information is also stored in Australia. From 8 October 2026, and before any school's staff sign in for the first time, authentication is provided by Microsoft Entra External ID with Australian data residency and two-factor codes are delivered through Azure Communication Services. We will not give any school access to the Platform until both are in place.

Our business email and file storage run on Microsoft 365 and Microsoft OneDrive with Australian data residency. Source data used to prepare reports outside the Platform is held there.

6.2 Our own business records

Our customer relationship management system (HubSpot) holds work contact details for school staff, being name, role, school, work email and work phone, together with correspondence and records of our dealings with a school. It holds **no student data, no School Data and no Platform account or credential data.**

Our HubSpot account is hosted in HubSpot's Australian data centre in Sydney, so these records are stored in Australia and are replicated for backup only within the Australian hosting region.

HubSpot, Inc. is nonetheless a United States company, and its published terms state that in limited circumstances its personnel, affiliates or sub-processors outside Australia may access or process account data for customer support, to investigate a security incident, for product development, and for usage analytics, which HubSpot transfers to the United States. That access is limited to the work contact details and correspondence described above. Our commitment that data never leaves Australia applies to School Data and to Platform account information, neither of which is held in this system, and that commitment is unaffected.

7. WHO WE DISCLOSE INFORMATION TO

We disclose School Data to no one, other than:

- the school it belongs to;
- the service providers listed below, which store or process it on our behalf under contracts requiring equivalent protections; and
- where required by law, a court or a regulator, in which case we will notify the school first unless legally prohibited from doing so.

7.1 Service providers that handle School Data or Platform account information

Each provider below processes the information on our behalf as a service provider under contract, in accordance with the Australian Privacy Principles and, where the customer is a NSW government school, the Information Protection Principles. That is the lawful basis on which each processes the information.

Provider and contact	Purpose	Information held	Location
Microsoft (Azure) Microsoft Pty Ltd www.microsoft.com/en-au/privacy	Hosting, database, storage and backup for the Apex Platform	School Data	Australia
Microsoft (365 and OneDrive) Microsoft Pty Ltd www.microsoft.com/en-au/privacy	Business email and file storage	Correspondence with school staff; source data used to prepare reports outside the Platform	Australia
Microsoft (Entra External ID) In place from 8 October 2026 Microsoft Pty Ltd www.microsoft.com/en-au/privacy	Authentication and staff account records	Staff name, email address, mobile phone number, credential and sign-in metadata. No student data.	Australia

Provider and contact	Purpose	Information held	Location
Microsoft (Azure Communication Services) In place from 8 October 2026 Microsoft Pty Ltd www.microsoft.com/en-au/privacy	Delivery of two-factor authentication codes by SMS, and delivery of Apex's own security and system notification emails	Staff mobile phone number and the verification code; recipient email address and the content of security and system notifications. No student data.	Australia

We will notify our school customers at least 30 days before adding or changing any provider that would have access to School Data, and they may object.

7.2 Providers that handle our own business records only

The provider below does not handle School Data. It is not a sub-processor of School Data and does not appear in Annexure A of our Terms of Service.

Provider and contact	Purpose	Information held	Location
HubSpot HubSpot, Inc. www.hubspot.com/data-privacy/privacy-policy	Customer relationship management and marketing	Names, roles, schools and work contact details of school staff, and correspondence. No student data, no School Data and no Platform account or credential data.	Australia (Sydney), with limited offshore access (see 6.2)

HubSpot processes this information on our behalf as a service provider under contract, in accordance with the Australian Privacy Principles.

8. SECURITY

The Apex Platform is being prepared for service commencement in Term 4, 2026. We distinguish below between what is in place now and what we have committed to have in place before any school begins using the Platform. Every commitment carries a date.

In place now

- All student data stored and processed in Australia, on Microsoft Azure in Australian regions
- Encryption in transit: TLS 1.3 and 1.2 only, with older protocols disabled. The Platform holds a Qualys SSL Labs rating of A+
- HTTP Strict Transport Security enabled
- Role-based access control, with production access restricted to named individuals, reviewed at least every six months and on any change of role or departure
- Logical separation between each school's data
- Automated tests verifying that a user belonging to one school is refused access to another school's data, forming part of the platform's automated test suite
- No real school data is ever used in development or testing. These environments use synthetic data only

- Logging of sign-in events
- Automated scanning for vulnerable code libraries and for credentials committed to source control
- Critical security patches applied within 14 days
- A documented Data Breach Response Plan, reviewed at least annually, covering privacy, security and online safety incidents, with every incident recorded in an incident register
- A documented Business Continuity and Disaster Recovery Plan, reviewed at least annually, with a summary available to schools on request

Committed by 8 October 2026, before any school begins using the Platform

- Two-factor authentication required for every staff account, by one-time code delivered by SMS to a nominated mobile number
- Authentication moved to Microsoft Entra External ID, with staff account records held in Australia
- Two-factor code delivery moved to Azure Communication Services, processed in Australia
- Encryption at rest for the database, file storage and backups
- A separate production environment, maintained separately from development and test, in Australian Azure regions
- Automatic backups taken by the Azure hosting platform on a confirmed and documented daily schedule, encrypted at rest, held in Australian Azure regions, with a documented retention period no longer than 90 days
- A documented test of restoration from backup, repeated at least annually thereafter, with the date and outcome of the most recent test available to schools on request
- Secrets and credentials managed through Azure Key Vault
- Logging of access to, and export of, student data
- Automated alerting on unusual activity, including repeated failed sign-ins and bulk data export
- A web application firewall in front of the Platform, restricting access to network addresses within Australia and limiting the rate of requests from any single address, and Microsoft Defender for Cloud enabled
- A documented system and database hardening baseline, covering default accounts, unnecessary services, permitted ports and protocols, and the end-user devices used to administer the Platform, reviewed at least annually
- File upload controls following the principles of the OWASP File Upload Cheat Sheet, including verification of file type and file signature, sanitisation of file names, size limits, and scanning for malicious content
- The Platform database reachable only over a private network endpoint, with no public network endpoint
- Completion of recognised cyber security awareness training by every individual with access to School Data, with the completion date recorded, repeated at least annually

- OWASP ASVS v5.0.0 Level 1 adopted as our application-security engineering and verification baseline
- Cyber liability insurance

Committed by 1 July 2027

- Independent penetration testing of the Platform, with a summary report available to schools on request
- A vendor-managed rule set based on the OWASP Core Rule Set applied to the web application firewall, in addition to the rules described above

We are undertaking a Safer Technologies for Schools (ST4S) assessment, the schools sector assessment administered by Education Services Australia. No badge has been awarded. We hold no independent security certification of our own. Microsoft Azure separately holds certifications covering the infrastructure we run on; those apply to Microsoft's infrastructure, not to our own practices, and we do not claim them as ours.

9. DATA BREACHES

If a data breach affects a school's information, we will:

- notify the school within 24 hours of becoming aware of it;
- provide details of what occurred, what information was involved, and the steps we are taking;
- provide the information the school requires to meet its own reporting obligations, including under the NSW Mandatory Notification of Data Breach scheme; and
- not notify individuals, the public or a regulator about a school's data without first consulting the school, unless required by law.

Every privacy, security or online safety incident is investigated, remediated and recorded in our incident register, whether or not it meets the threshold for notification.

10. HOW LONG WE KEEP INFORMATION

Where a period below runs from the end of a subscription, it is measured from the **Deletion Start Date**, being the date of the written notice or written confirmation of termination, or the date of expiry, whichever applies.

Information	Retention period
School Data	For the duration of the school's subscription. From the Deletion Start Date, available for export for 30 days, deleted from production systems within 60 days, and cleared from backups in accordance with our backup rotation cycle, being no longer than 90 days. Deletion confirmed in writing on request.

Information	Retention period
Platform account records, including mobile phone number held for two-factor authentication	For the life of the account, then 12 months. A staff member may remove or change their nominated number at any time.
Correspondence	Indefinitely
Contact records for schools we have approached	Indefinitely, or until the contact asks us to remove them
Financial and tax records	7 years, as required by law

11. ACCESS, CORRECTION AND MARKETING

Students, parents and carers. Requests to access or correct information a school holds should be made to the school, which has its own process. We assist schools to respond at no charge.

Everyone else. If we hold your information directly, you can ask us to tell you what we hold, provide a copy, correct it, or delete it where we are not required to retain it.

Email admin@apexdatasolutions.com.au. We will confirm your identity and respond within 30 days. There is no charge.

Marketing. To stop receiving marketing from us, use the unsubscribe link in any email or reply and tell us.

12. COMPLAINTS

If you believe we have mishandled your information, contact us at admin@apexdatasolutions.com.au. We will acknowledge within 5 business days and respond within 30 days.

If you are not satisfied with our response, you can escalate it to:

- the **Information and Privacy Commission NSW**, ipc.nsw.gov.au, 1800 472 679, for matters concerning information we handle for a NSW government school; or
- the **Office of the Australian Information Commissioner**, oaic.gov.au, 1300 363 992.

You may contact either regulator directly without first raising the matter with us.

13. OUR WEBSITE AND THE PLATFORM IN YOUR BROWSER

No analytics, tracking or advertising. The Apex Platform runs no web analytics, no tag manager, no advertising or remarketing tag, no social media pixel and no third-party chat widget. We do not profile you, we do not track you across other websites, and we do not sell or share information about your visit with anyone for marketing. There is nothing on the Platform whose purpose is to observe you.

Cookies and browser storage. We do not set cookies for analytics or advertising. To keep you signed in, the Platform issues a session token. It holds no assessment data, and signing out clears it. By 8 October 2026, and before any school begins service, that token is held in a secure server-side session cookie set by the Platform and is not stored in your browser at all. Until that change takes effect, the token may be held in your browser's own local storage, where it is readable only by the Platform. Because we set no analytics or advertising cookies, there is no consent banner to click through. There is nothing to consent to.

Fonts and code libraries. Like most web applications, the Platform uses standard typefaces and code libraries. By 8 October 2026, and before any school begins service, these files are served from Apex's own Australian infrastructure and the external requests stop, with an automated build check that fails if any page requests a file from an external network. Until that change takes effect, your browser may request some of these files directly from a third-party network, some of which operate outside Australia. Where it does, that network can see your IP address, your browser and device type and the time of the request, as a technical consequence of delivering a file. No account details, no school information and no student data are sent, and none of these providers is given anything that identifies you to us.

Student data is not affected by any of this. Nothing in this section applies to School Data. Assessment data is stored solely in Australia as described in section 6, is never sent to an analytics provider or a content delivery network, and never leaves the Platform through your browser.

Our public website. Our public website at www.apexdatasolutions.com.au is served from Apex's own infrastructure on Microsoft Azure in Australia. It is not hosted on any third-party website platform. We set no analytics or advertising cookies on it and we do not record visitor statistics.

Forms. If you complete a form on our website, the details you provide are used to respond to you and are handled as described in section 4.

14. CHANGES TO THIS POLICY

We may update this policy. Updates will carry a new version number and effective date and will be published at www.apexdatasolutions.com.au/privacy.

We will notify our school customers directly at least 30 days before any change to this policy takes effect.

15. CONTACT

Apex Data Solutions Pty Ltd ABN 71 670 512 857 13 Draper Avenue, Roselands NSW 2196
admin@apexdatasolutions.com.au