Data Processing Agreement

How Clarity4Growth processes school data under Australian privacy law. Last updated: April 2026.

This DPA is ready to sign. Download the PDF, fill in your school details, and return a signed copy to privacy@clarity4growth.com.au.

Download DPA (PDF)

Parties

Controller: The School (data controller of all student information)

Processor: Clarity4Growth (ABN 51 567 672 559), provider of the EASY Compliance platform

1. Definitions

- **Personal Information** has the meaning given in the *Privacy Act 1988* (Cth)
- **Sensitive Information** has the meaning given in the *Privacy Act 1988* (Cth), including health information and information about a person's disability
- **Processing** means any operation performed on Personal Information
- **APPs** means the Australian Privacy Principles in Schedule 1 of the *Privacy Act 1988* (Cth)

The School is the **data controller**. Clarity4Growth is the **data processor**, acting only on the documented instructions of the School.

Clarity4Growth will not use Personal Information for its own purposes including marketing, profiling, model training, or product analytics.

---

3. Subject matter and duration

- **Subject matter:** processing of student, parent/carer, and staff data for the purpose of NCCD compliance recording, student support planning, and reporting
- **Duration:** for the term of the service agreement plus the retention period in Section 9
- **Data subjects:** students enrolled at the school, their parents/carers, and the school's teaching and support staff

---

4. Data residency

All Personal Information is processed and stored in **Australia only** (Google Cloud, Sydney region). No data is transferred outside Australia at any time, including for AI processing, backups, or support.

---

5. Sub-processors

Sub-processor	Purpose	Location	Certification
Google Cloud Platform	Hosting, database, storage, backups	Sydney, Australia	ISO 27001, SOC 2 Type II, IRAP PROTECTED

Google Vertex AI	AI features (optional, names removed)	Sydney, Australia	Same as above; no training on customer data
Sentry (optional)	Error monitoring (anonymised)	EU (data de-identified before transmission)	SOC 2 Type II

The School will be notified at least 30 days in advance of any new sub-processor.

---

6. Security measures

Encryption

- TLS 1.2+ for all data in transit
- AES-256 encryption at rest (Google Cloud default)

Access control

- Role-based access enforced server-side via Firestore security rules (verified by automated tests)
- Per-school OAuth 2.0 client with Google Workspace domain restriction
- Multi-factor authentication for all Clarity4Growth administrative access

Audit logging

- Every read, write, and delete on student records is logged with timestamp, user ID, action type, and target document
- Audit logs are append-only and retained for the life of the school

AI safeguards

- All student names, parent names, staff names, emails, phones, and DOBs are replaced with placeholders on the user's device before any AI request
- AI requests are routed through Vertex AI in Australia only
- Vertex AI does not use customer data for model training (Google's contractual commitment)

- Encrypted at rest, same Australian region

Vulnerability management

- Dependency scanning on every commit
- Critical patches within 24 hours, high within 7 days
- Vulnerability disclosure: security@clarity4growth.com.au

---

7. Breach notification

In the event of a data breach, Clarity4Growth will:

1. Notify the School within **24 hours** of becoming aware
2. Provide all available information about the nature, scope, and consequences
3. Document the breach and remedial actions
4. Cooperate with the School's notification obligations under the *Privacy Act 1988* Notifiable Data Breaches scheme

---

8. Data subject rights

Clarity4Growth will assist the School in responding to access, correction, and deletion requests within 14 days. Built-in tools support single-student export (JSON + PDF), cohort export, permanent deletion, and audit log review.

---

9. Retention and deletion

- **30-year retention** is the default (NCCD evidentiary requirements)
- Records can be archived (locked, read-only) when a student leaves
- On termination: data returned in machine-readable format OR deleted within 30 days, at the School's choice

The School may, on reasonable notice and not more than once per year:

- Review the most recent penetration test report
- Review Firestore security rules and test coverage
- Request an audit log summary for any student
- Engage an independent tester at the School's cost

---

11. Insurance

Clarity4Growth maintains:

- Professional Indemnity insurance (minimum £1,000,000)
- Cyber Security insurance
- Public Liability insurance (minimum £1,000,000)

---

12. Governing law

This DPA is governed by the laws of Victoria, Australia.

Signatures

Signed for the School:

Name: _____

Title: _____

Date: _____

Signed for Clarity4Growth:

Name: _____

Title: _____

Date: _____

This template is provided as a baseline. Both parties should review with legal counsel before signing.