

Edsthetic

Less administration. More teaching.

Writeiq

Security and Privacy Overview

*A reference document for Australian schools,
IT Coordinators, and Privacy Officers
preparing a Privacy Impact Assessment for Writeiq.*

Issued by Edsthetic · ABN 70 939 441 240

Document version 1.7 · 26 July 2026

Privacy and security enquiries: legal@edsthetic.com.au

1. Purpose of this document

This document is provided to schools considering or implementing Writeiq, the English writing assessment platform from Edsthetic. It is intended to give schools and their privacy and IT teams the technical and operational information they need to confidently complete their own Privacy Impact Assessment for Writeiq, and to satisfy themselves that the platform meets the privacy and security expectations of the Department of Education.

Edsthetic does not complete or sign Privacy Impact Assessments on behalf of schools. The PIA remains the school's responsibility, as required by departmental policy. This document provides the underlying facts the school needs to populate the PIA accurately, including data hosting, encryption, authentication, sub-processors, retention and security testing posture.

The document is written in plain English, with technical terms explained the first time they appear. Where useful, simple analogies are used. A glossary is provided in Section 18.

Should anything be unclear, or should you require further evidence to support a specific PIA control, please contact us at legal@edsthetic.com.au. We respond to school privacy enquiries within two working days.

2. Executive summary

Writeiq is an English writing assessment platform designed and operated entirely from Australia. The platform is hosted in Sydney, all data is encrypted both in storage and in transit, and every school's data is logically separated from every other school's at the database layer. Edsthetic does not sell, trade, or share student data with any third party. The platform's third-party sub-processors are limited to a small set of well-established providers, each of which has its own contractual and regulatory protections in place.

In summary, Writeiq:

- Stores all customer data in Sydney, Australia, under a data residency commitment. The database infrastructure is provided by Supabase, Inc. and runs on AWS Sydney (ap-southeast-2) — the same AWS region that hosts Australian Government and major Australian bank workloads.
- Encrypts data both at rest (AES-256) and in transit (TLS 1.2 or higher across all browser, app, and server connections).
- Authenticates every staff member with their own login. Time-based One-Time Password (TOTP) multi-factor authentication is in place — required for school administrators and optional for teachers. Single Sign-On via Google Workspace or Microsoft 365 is available for staff and inherits the school's MFA policy. Students do not require email accounts; see Section 7.2.
- Enforces strict per-school data separation at the database level using Row-Level Security, a PostgreSQL feature that prevents one school's users from ever seeing or accessing another school's records.
- Routes all public traffic through Cloudflare, which provides Web Application Firewall protection, DDoS mitigation, and bot management.
- Uses Claude models running on Amazon Bedrock inside the Australian boundary (AWS Sydney and Melbourne) for AI-assisted feedback and analysis, under a Data Processing Addendum that prohibits the use of customer data to train AI models. For typed submissions, only the writing text and rubric are transmitted — no student names, identifiers, or school details. For handwritten scans, the image is transmitted as scanned (any name the student wrote on the paper is visible); schools can opt to use

student UIDs instead of names on paper, and Edsthetic is trialling automated cropping of names from scans for Term 3 2026. See Section 10.2 for full disclosure.

- Supports bulk school onboarding via CSV import and OneRoster 1.2 ZIP bundles from the school's management system (Compass, Edval, Sentral, Edumate, and others). Inbound CSV and ZIP files are parsed entirely in the school administrator's browser and are never transmitted to Edsthetic's servers in raw form. See Section 7.5.
- Maintains an audit log of every sign-in event and administrative action, retained for at least twelve months.
- Completed an OWASP ZAP passive manual exploration of production (not an active penetration test); no High-risk issues were identified, and SRI hardening and app-host cookie scoping were confirmed closed on the 24 May 2026 passive re-scan. In-place Playwright real-browser regression testing. Forward roadmap: active OWASP ZAP DAST of staging before each commercial deployment and at least quarterly; Safer Technologies for Schools (ST4S) Readiness Check submission in Term 3 2026; an external manual penetration test in 2027; and SOC 2 Type II certification by 2028.

Plain-English bottom line: Writeiq is built and run in Australia, every school's data is kept separate from every other school's, no human or AI uses student writing for any purpose other than producing feedback for that school, and we are working steadily towards every external assurance the Department recognises.

3. About Edsthetic

Edsthetic is an Australian partnership (ABN 70 939 441 240) building software for Australian schools. The business is based in Victoria. Edsthetic operates two products: Writeiq, the English writing assessment platform described in this document, and Allocateiq, a separate platform for learning support allocation.

Edsthetic was founded by Australian educators who continue to work in Australian schools. The platforms are designed from the ground up around the way Australian schools actually operate, with explicit support for the Victorian Curriculum, the Australian Curriculum (AC9), state syllabi, the IB Middle Years Programme, VCE, NSW NESA, QCAA, WASCSEA, the UK National Curriculum, and the IB Primary Years Programme.

Edsthetic is bound by the Australian Privacy Principles under the Privacy Act 1988 (Cth), and by relevant state privacy law (including the Victorian Information Privacy Principles) where it holds personal information about residents of those jurisdictions.

4. About Writeiq

Writeiq is an English writing assessment platform for Years 3 to 12. It supports teachers, school leaders, and students with three primary functions: AI-assisted, IWAF-aligned feedback and teacher-reviewed scoring support on student writing, generating follow-up teaching resources informed by that feedback, and surfacing whole-school analytics on writing performance over time.

Who uses Writeiq

- **Teachers** — to mark student writing, give per-criterion feedback, generate writing-focused lessons, and view class progress.
- **School leaders** — to view school-wide and year-level analytics on writing performance and growth.

- **School administrators** — to manage staff and student accounts, configure settings, and access cost and usage reports.
- **Students** — to receive feedback on their writing, view their progress, and (optionally) submit work for marking via supervised classroom sessions.

What information Writeiq holds about students

Writeiq is deliberately designed to hold the minimum information needed to fulfil its purpose. The information Writeiq holds about each student is limited to:

- First name, last name, year level.
- A school-issued unique identifier (such as a CASES21 ID), used solely to disambiguate students with similar names.
- The class or classes the student belongs to.
- Writing submissions (which may be typed by the student or scanned and transcribed from handwritten work) and the assessment feedback generated for those submissions.

Writeiq does not collect or store: addresses, contact phone numbers, parent contact details, dates of birth, photographs of students, medical or health information, behaviour records, attendance records, financial information, or family circumstance information. Writeiq is not a school management system and does not function as one.

5. Where data is stored

5.1 Hosting location and jurisdiction

Detail	Description
Hosting region	Sydney, Australia (AWS ap-southeast-2)
Data residency	All customer data is stored in Australia under a data residency commitment, and is not replicated, mirrored, or backed up to any non-Australian location.
Hosting provider	Supabase, Inc., a managed PostgreSQL database provider headquartered in San Francisco. The Sydney AU region used by Writeiq is operated entirely on AWS infrastructure in Sydney.
Underlying data centre operator	Amazon Web Services (AWS) ap-southeast-2 region. AWS Sydney facilities are ISO/IEC 27001 certified and host data for Australian Government, banking, and university customers.
Legal jurisdiction over data hosted in Sydney	Australian Commonwealth and Victorian state law apply to data physically held in Australia.
Legal jurisdiction over Edsthetic	Australian Commonwealth and Victorian state law.
Cross-border data transfer for storage	None. All storage is in Australia. Data Processing Addendum with Supabase incorporates Standard Contractual Clauses providing additional protection.
Cross-border data transfer for processing	None for student writing. Since 25 July 2026 AI-assisted feedback, scoring support and handwriting transcription run on Amazon Bedrock inside the Australian boundary (Sydney ap-southeast-2 / Melbourne ap-southeast-4), and handwriting layout extraction for the optional Vision feature runs in Azure Australia East. See Section 10. Before that date, model processing ran on the Anthropic API in the United States under a no-training, no-retention DPA. The only remaining cross-border processing is operational telemetry (Sentry, PostHog), which carries no student writing or names.

5.2 What is Supabase, in plain language

Supabase is the company that provides the database that holds Writeiq's data. The Department of Education will not have encountered Supabase under that name before, but the underlying technology is one of the most widely used database systems in the world. The following summary explains what Supabase is and why it is appropriate for Australian schools.

- **Supabase, Inc.** is a managed database provider headquartered in San Francisco, USA. The actual customer data resides not at Supabase's office but in the AWS Sydney region (ap-southeast-2), under a contractual data residency commitment that prevents it from being moved out of Australia.
- This same arrangement (US-incorporated cloud provider, Australian data residency) is the model used by every major school SaaS vendor including Compass, Sentral, Education Perfect, and ClassDojo. It is also how Australian banks, government departments, and the major Australian universities use Microsoft Azure, AWS, and Google Cloud.
- The actual database product is **PostgreSQL**, an open-source database that has been used for over thirty years by organisations including the Australian Bureau of Statistics, the New York Times, Apple, and Reddit. PostgreSQL is widely regarded as one of the most secure and mature database systems available.
- **AWS Sydney holds ISO/IEC 27001 certification**, the international standard for information security management. AWS Sydney hosts data for the Australian Federal Government, the major Australian

banks, and many Australian universities.

- **Supabase, Inc. holds SOC 2 Type II certification**, an independent audit standard that verifies a vendor's controls over the security, availability and confidentiality of customer data over a period of time. Supabase publishes its trust and compliance posture publicly at supabase.com/security.
- Edsthetic's commercial contract with Supabase is governed by a **Data Processing Addendum (DPA)** signed in April 2026, which incorporates Standard Contractual Clauses (Module Two: controller to processor) for international data protection. Under the DPA, Supabase commits contractually to: keep customer data primarily processed in the geographical region directed by Edsthetic (Sydney AU); notify Edsthetic of any Security Incident within 48 hours; delete all customer data within 30 days of contract termination; conduct regular penetration testing of its infrastructure by reputable third-party security firms; and grant Edsthetic annual audit rights over its compliance with the DPA. The signed DPA is on file and available to schools on request.
- One point of additional reassurance for Australian schools: **Atlassian Corporation Plc** (Level 6, 341 George Street, Sydney NSW), an Australian-listed company, is among Supabase's own sub-processors (used for status page services). The supply chain therefore includes Australian-based providers as well as US-based providers.
- The Supabase **Transfer Impact Assessment (TIA)**, available alongside the DPA, documents that Supabase has never disclosed customer data to law enforcement under FISA 702 or EO 12333. Both the DPA and TIA are available to schools on request to legal@edsthetic.com.au.

In short: when a school uses Writeiq, their data lives in Sydney, in a PostgreSQL database, on AWS infrastructure that meets the same standards relied upon by Australian Government agencies, under a contract that prevents the data leaving Australia.

5.3 The shared-database question

Schools sometimes ask whether Writeiq operates a separate database for each school. It does not. Writeiq operates a single PostgreSQL database shared across all customer schools. This is industry-standard architecture for school software products and is the same model used by Compass, Sentral, ClassDojo, Education Perfect, and the great majority of cloud-based education products.

What protects each school's data from every other school's is not physical separation, but a feature of PostgreSQL called **Row-Level Security**. The simplest way to think about this is by analogy:

Imagine an apartment building in Sydney. Every school is an apartment in that building. Each apartment has its own lock, its own key, and its own residents. The neighbours cannot see, hear, or enter another apartment, even though they share a building, because each door enforces its own access rules. Row-Level Security is the database equivalent of that locked door. Every single request the database receives is checked against a rule that confirms the user is allowed to see that data. If the user does not belong to the school that owns the row, the database returns nothing, as if the data did not exist.

Row-Level Security is enforced inside the database itself, not at the application layer. This is important: even if a software bug were introduced in Writeiq's code that tried to read data across schools, the database itself would refuse the request. The protection is at the deepest possible layer of the system.

In addition to Row-Level Security, Writeiq uses what database engineers call **SECURITY DEFINER** functions, which add a second authorisation check. Every read and write that touches school data is filtered by both controls.

6. Encryption

All data Writeiq handles is encrypted at every stage of its life. There is no point at which student writing or staff information is held in plain text on a network or on disk.

Layer	Protection
In transit (network)	TLS 1.2 or higher with modern ciphersuites on every connection between the user's browser and Writeiq, and between Writeiq and any sub-processor (Supabase, Amazon Web Services, Microsoft Azure, Cloudflare, Sentry, PostHog). TLS 1.2+ is the current internet standard for encrypted connections, and is the same protocol used by every major Australian bank for online banking.
At rest (database)	AES-256, the encryption standard used by the Australian Government for protected information. Supabase encrypts data at rest using AES-256 with encryption keys protected by FIPS 140-2 compliant Hardware Security Modules (HSMs) — the same standard used by the US Government for classified information.
At rest (backups)	AES-256, applied automatically to every backup. Backups for the Sydney AU project remain in the AWS Sydney region under the same encryption controls as the live database.
Session cookies	All session cookies are marked HttpOnly (cannot be read by client-side code), Secure (only sent over HTTPS), SameSite=Strict (cannot be sent on cross-site requests, preventing entire categories of attack), and host-scoped to app.writeiq.com.au.
Browser storage	The Writeiq school-facing application does not write authentication tokens to <code>localStorage</code> or <code>sessionStorage</code> . JWT session tokens are held in HttpOnly cookies (see Session cookies above) and OAuth tokens are held in browser memory for the duration of the SSO callback only.
Inbound CSV / OneRoster ZIP files	Uploaded by school administrators for bulk import. NOT transmitted to Edsthetic servers — parsed entirely in the administrator's browser. Only the parsed and validated row data crosses the network. The raw file is never persisted server-side. Browser-side memory only, cleared on page reload. See Section 7.5.
Passwords	Staff email/password authentication is handled by Supabase Auth; Edsthetic never stores or sees a staff password, and no staff password hash is held by Edsthetic. TOTP recovery codes are hashed with PBKDF2-SHA-256 (600,000 iterations, per-code salt).
Authentication tokens	JWT session tokens are issued by Edsthetic's server and delivered as HttpOnly, Secure, SameSite=Strict cookies host-scoped to app.writeiq.com.au. OAuth access tokens received during SSO sign-in are held in browser memory for the duration of the callback only and are never persisted to <code>localStorage</code> or <code>sessionStorage</code> . Tokens are signed with HMAC-SHA256 using a secret known only to Edsthetic's server.

7. Authentication: who can sign in, and how

Writeiq's authentication system was rebuilt during May 2026 so that every staff member has their own per-user login. The previous per-school shared-PIN and licence-key model has been retired as a staff authentication path; staff now authenticate only via per-user email/password (handled by Supabase Auth) or SSO. Students have a separate access model — see Section 7.2.

7.1 Staff and school administrators

Every staff member at a school using Writeiq has their own individual account. Staff members can sign in by either of the following methods:

- **Email and password** — the staff member's school email address and a password set at first login. Authentication is handled by Supabase Auth; Edsthetic never stores or sees the password.
- **Single Sign-On (SSO)** — the staff member can choose to sign in with their school's Google Workspace or Microsoft 365 account. SSO is supported by industry-standard OAuth 2.0 with PKCE, and the school's identity provider remains the source of truth for authentication.

When a staff member signs in via SSO, Edsthetic never sees or stores the staff member's Google or Microsoft password. The school's identity provider tells Edsthetic only that the user has been successfully authenticated, and provides a short-lived signed token confirming their email address.

7.2 Students (PIA-critical)

Students do **not** require email accounts, passwords, or Single Sign-On to use Writeiq. This is a deliberate design decision. Many primary and lower-secondary students do not have school-issued email; mandating email would exclude them and create privacy overhead the assessment use case does not need.

Three student-access paths are available, ranked from most recommended to least:

- **Class Links** (*recommended*). Each class has a unique signed URL minted by the school administrator. Students click the link or scan its QR code to enter Writeiq directly. The link itself is the credential — it is signed and scoped to a specific school and class, and the school administrator controls its expiry. No student account exists in the authentication system; the link is the access token.
- **Student Access Code**. A school-set code (for example, ENG7A or RIVER2026) that students type once per device on the Student Gate. Administrators rotate the code by archiving the prior task and issuing a new code for the next assessment. Codes do not auto-expire on a fixed schedule, by design, so that a marking task started in one lesson can be completed in the next.
- **SSO (opt-in)**. Schools with mature student identity infrastructure (Google Workspace for Education, Microsoft Entra ID) may enable student SSO. This is opt-in per school. When enabled, students sign in with their school identity; Writeiq receives only an opaque OAuth token validated through the school's identity provider.

The `public.students` table stores student demographic data (first name, last name, year level, optional parent contact email, class assignments) but contains **no authentication fields** — no password hashes, no TOTP secrets, no `auth.users` foreign key. The optional email column is intended only for parent contact (for example, end-of-task report PDF delivery) and is never used for student sign-in. This architecture is preserved across all bulk data operations described in Section 7.5: importing student data via CSV or OneRoster populates demographic and class-assignment data only, and does not create authentication identities for those students.

Regardless of which access path the school chooses, students do not see or interact with other schools' data, other classes' data within their own school, or other students' work.

7.3 Multi-factor authentication

Multi-factor authentication via Time-based One-Time Password (TOTP) is available for staff. TOTP is compatible with Google Authenticator, Microsoft Authenticator, Authy, 1Password, and any other authenticator app that follows the RFC 6238 standard. MFA is optional for teachers at school discretion and required for school administrators.

In addition, schools using Google Workspace or Microsoft 365 Single Sign-On benefit from any MFA policy enforced by their identity provider, because Writeiq trusts the identity provider's authentication outcome. A school that mandates MFA at the Google or Microsoft level automatically extends that protection to Writeiq sign-ins.

7.4 Audit logging

Every sign-in attempt, successful or failed, is recorded in an audit log table along with the timestamp, source IP address, user agent, and authentication method. Every administrative action (creating an account, changing a role, removing a user, committing a bulk import) is also recorded. The audit log is retained for at least twelve months and can be exported on request to a school's IT or compliance team.

7.5 Account provisioning (per-user, CSV, and OneRoster)

Schools provision Writeiq accounts in one of two complementary ways. Both paths are gated by the school administrator and audit-logged.

Per-user invitations

The first school administrator is provisioned by Edsthetic during onboarding. That administrator invites additional users from the Users tab in the admin panel. Each invitation is an email, role, optional faculty, and optional class assignments. The invitee receives a unique claim URL (valid for 7 days by default) by email, delivered via Amazon SES in the Sydney region. They set their own password — or sign in via SSO if their email matches their Workspace or Entra account. Removal is a soft-delete: the user can no longer sign in, but their submission history is preserved for audit purposes.

Bulk data import (CSV)

For schools with established staff and student rosters in their school management system, the administrator may bulk-import classes, staff, and student data via the Settings → Data import tab. Three import types are supported: classes (code, year level, display name); staff (email, name, role, faculty, class assignments); and students (demographic data, no authentication fields, as described in Section 7.2). Each import workflow has three stages:

- **Parse.** The CSV is parsed *entirely client-side* using the established PapaParse library. **The raw CSV file is never transmitted to Edsthetic's servers** — only the parsed and validated row data is sent to the import RPC. This means a CSV containing accidental clipboard contents, hidden columns, or formatting artefacts never reaches the server in its raw form.
- **Dry-run.** A Postgres function validates every row against the schema, computes the diff against existing data (rows to insert, update, leave unchanged, archive, unarchive), and returns errors and warnings. No changes are committed at this stage. The administrator reviews the diff before deciding to commit.
- **Commit.** If the dry-run produced no errors (and any warnings have been explicitly acknowledged by the administrator), the changes are applied in a single transaction. The commit honours the chosen mode: *merge* (default — add new rows, update existing, leave non-matching rows alone) or *replace* (rows present in existing data but absent from the upload are archived). Every commit writes an entry to the audit log.

OneRoster 1.2 ZIP bundles

The Data import tab additionally accepts OneRoster 1.2 CSV bundles — the standard export format produced by Compass, Edval, Sentral, Edumate, and most other Australian school management systems. The ZIP is extracted entirely client-side using the JSZip library; the constituent CSVs (`users.csv`, `classes.csv`, `enrollments.csv`) are parsed and normalised into the three import formats described above. **The raw ZIP is never transmitted to Edsthetic's servers.**

The OneRoster pre-processor explicitly filters:

- Only rows with `status=active` are emitted.
- Only year levels 3–13 (Writeiq's supported range) are emitted. Pre-K and primary years 1–2 are skipped with a warning surfaced to the administrator.
- Role mapping: OneRoster *student* becomes our student; *teacher* and *aide* become teacher; *administrator* becomes `school_admin`; *parent*, *guardian*, *proctor*, and *relative* are silently filtered out, never imported.

Source row counts and a complete warnings list are presented to the administrator before any commit decision, so the diff between the source bundle and the committed data is transparent.

8. Authorisation: what each user can see and do

Authorisation determines what a signed-in user is allowed to access. Writeiq enforces authorisation at three independent layers, so that a failure or bug in any one layer is caught by the others.

Layer	How it works
Application layer	Edsthetic's server-side code checks every request to confirm that the user holds a valid session, that the session has not expired, and that the user has a role that permits the action.
Database function layer	Every read or write to school data goes through a <code>SECURITY DEFINER</code> function which compares the user's authenticated identity to the school the data belongs to.
Row-Level Security	PostgreSQL itself rejects any query that asks for data outside the user's school, regardless of where the query came from. This is the deepest layer and operates inside the database engine.

8.1 Role-based access within a school

Role	Access
School Administrator	Full access to staff, classes, students, and licensing settings within their school. Cannot see any data belonging to any other school.
School Leader	Read access to school-wide analytics, year-level breakdowns, and submission data within their school. Cannot edit student records or change settings.
Teacher	Access to their own classes and the students enrolled in them. Can mark, comment, and generate feedback. Cannot see classes they are not assigned to.
Student	Access to their own writing submissions and feedback. Cannot see other students' work, even within their own class.
Edsthetic Founders / Engineers	Production access is limited to two named individuals, used only for incident response, scheduled maintenance, and customer support. All access is logged. Edsthetic personnel do not browse or read school content as part of normal operations.

9. Network and edge protection

All traffic to and from Writeiq passes through Cloudflare's global edge network. Cloudflare is one of the largest network security providers in the world, protecting more than twenty per cent of all websites on the public internet, including the Australian Government's primary online services portal, Australia Post, and the major Australian banks.

What Cloudflare provides Writeiq

- **Web Application Firewall (WAF)** — automated detection and blocking of common attack patterns including SQL injection, cross-site scripting, and request smuggling. The WAF rule set is updated by Cloudflare in response to new threats, automatically, with no action required from Edsthetic.
- **Distributed Denial of Service (DDoS) protection** — Cloudflare absorbs and filters out volumetric attacks at the edge, before they reach Writeiq's servers. Cloudflare's network has handled the largest DDoS attacks ever recorded.
- **Bot management** — automated traffic from scrapers, credential-stuffing bots, and content harvesters is identified and rate-limited or blocked.
- **TLS termination at the edge** — every connection is encrypted from the user's browser all the way to Cloudflare, then re-encrypted from Cloudflare to Writeiq's servers. There is no point in the journey at which traffic is unencrypted.
- **Rate limiting** — additional rate limits are applied at the edge for sensitive endpoints (login, password reset) to prevent automated abuse.

From a school IT perspective, no firewall changes are required to use Writeiq. The platform is reachable on standard HTTPS port 443 and works with any school filtering or proxy product that allows access to general educational web traffic.

10. IWAF-aligned feedback and teacher-reviewed scoring support (Amazon Bedrock, Australia)

Writeiq's feedback and scoring support are AI-assisted and IWAF-aligned. Student writing is sent to a Claude model for analysis, which produces per-criterion feedback and a recommended score band. This is the only point at which student writing leaves Edsthetic's own infrastructure, and it does so under a written contract with strict data handling terms. Writeiq does not mark autonomously: the AI-assisted analysis is a recommendation, the teacher reviews it and remains the final decision-maker, and the final score is teacher-confirmed.

Since 25 July 2026 this processing happens in Australia. The Claude models run on Amazon Bedrock within the Australian boundary - AWS Sydney (ap-southeast-2) and Melbourne (ap-southeast-4) - so student writing does not leave the country at any stage. Before that date this one step ran on the Anthropic API in the United States under a contract with equivalent no-training and no-retention terms. Work marked before 25 July 2026 was processed under those terms, and that is stated here rather than removed.

10.1 Typed submissions: what is sent and what is not

For typed submissions (writing entered directly via keyboard, the most common case), the data Writeiq transmits to the model service is strictly limited. Edsthetic verified this end-to-end in code review during the May 2026 security pass, and again at the July 2026 move to Amazon Bedrock.

Sent to the model service:

- The writing text itself.
- The writing type (narrative, analytical, recount, persuasive, etc.).
- The year level (e.g., Year 9).
- The subject context (English, Humanities, Science, Health & PE, Arts, Technology, or other), used to tune the feedback voice to disciplinary conventions.
- The rubric and criteria to be applied.

NOT sent to Anthropic:

- Student first name or last name.
- Student identifier (CASES21 ID, school UID, or any other ID).
- Class name or class code.
- Teacher name.
- School name or school identifier.
- Any other student personal information.

The service receives the writing as anonymous text alongside the rubric. The piece of writing cannot be linked back to an individual student from the contents of the API call alone.

10.2 Handwritten scans: an honest disclosure

Writeiq supports handwritten work via scan upload (PDF or image). Schools and parents should understand how this differs from typed submissions in one important respect.

When students complete writing on paper, they conventionally write their first name and last name at the top of the page in their own handwriting, exactly as they have always done on paper-based assessment. When a teacher then scans the paper and uploads it to Writeiq, the resulting image contains whatever the student wrote on the paper, including that name.

Writeiq sends this scanned image to the model service in Australia for transcription, and the system prompt asks it to extract the handwritten name in order to match each transcript back to the correct student in the teacher's class list. In practical terms, this means: for handwritten submissions, the student's name as written on the paper is visible to the transcription service during that step, in the same way it would be visible to a relief teacher marking a paper-based stack. The service returns the extracted name as plain text along with the transcript, and Writeiq uses that name to attach the transcript to the correct student record. Neither Amazon Bedrock nor Azure Document Intelligence retains the image beyond the request; Edsthetic retains the image in Supabase Sydney AU under the same controls as all other student data. Since 25 July 2026 the image does not leave Australia at any point in this process.

Edsthetic believes this is the right level of transparency. Every comparable AI-assisted feedback platform that supports handwritten work (Edexia, Mark My Words, Brightpath when used with handwriting input) relies on the same mechanism, because this is how paper-based work has always identified its author. We

disclose it explicitly rather than hide it.

Two options for schools that prefer stricter privacy controls for scanned work

Option 1 (school-side, no technical change required): Schools can adopt a workflow where students write a school-issued numeric or alphanumeric identifier (a 'student UID') at the top of their paper instead of their first and last name. The teacher keeps the UID-to-name mapping in their own roster or in Writeiq's class list. This way, even the scanned image sent for transcription contains no recognisable personal identifier — only a code. This is at the school's discretion and requires zero change in Writeiq.

Option 2 (Edsthetic, on the roadmap and currently in trial for Term 3 2026): Edsthetic is trialling an automated pre-processing step that crops or redacts the top region of each scanned page before the image is sent for transcription. The redacted region is held only in Supabase Sydney AU. Edsthetic processes the cropped portion locally to extract the student name and match it to the class list, while sending only the redacted body of the writing to the transcription service. Once this trial completes successfully, it will become the default for all scans. Schools running early pilots may opt into the trial on request to support@edsthetic.com.au.

10.3 The contractual basis

Edsthetic's relationship with Amazon Web Services is governed by the AWS Customer Agreement, the AWS Data Processing Addendum, and the Amazon Bedrock service terms. Together these form a Data Processing Agreement between Edsthetic (as data controller) and AWS (as data processor). The protections relevant to schools are:

- Customer content submitted to Amazon Bedrock is **not used to train, improve, or evaluate** any model, whether AWS's own or a third-party model provider's.
- Amazon Bedrock **does not store prompts or completions**. Student writing is processed for the request and is not retained by the service afterwards.
- Customer content is **not shared with the model provider**. Anthropic personnel have no access to the inference infrastructure and do not receive the writing.
- AWS will **not use customer content** for any purpose other than providing the service, and will not sell or share it.
- AWS notifies Edsthetic of a Security Incident **without undue delay** after becoming aware of it.
- Customer content is encrypted with **AES-256 at rest and TLS 1.2 or higher in transit**.
- AWS maintains **SOC 2 Type II** and **ISO/IEC 27001** certification, and the Sydney region is **IRAP-assessed** for Australian government workloads. Current certifications are available through AWS Artifact.
- Because the processing is performed in Australia, **no Standard Contractual Clauses or other cross-border transfer mechanism is required** for it under APP 8.

10.3.1 The position before 25 July 2026 (historical)

Until 25 July 2026, model processing ran on Anthropic's Claude API in the United States, governed by Anthropic's Commercial Terms of Service and Anthropic's Data Processing Addendum effective 24 February 2025, publicly available at anthropic.com/legal/data-processing-addendum. That contract governs work marked before the cutover, and its protections are recorded here for that reason:

- Anthropic will **not 'sell' or 'share'** customer personal data, as defined under applicable data protection laws (DPA clause B.3.a).
- Anthropic will **not retain, use, or disclose** customer personal data outside the direct business relationship or for any purpose other than performing the Services (DPA clause B.3.b). Per Anthropic's Commercial Terms of Service, customer data is not used to train, improve, or evaluate Anthropic's AI models.
- Anthropic will not combine customer personal data with personal data received from any other source (DPA clause B.3.c).
- Anthropic will notify Edsthetic of any Security Breach within **48 hours** of becoming aware of it (DPA clause G.1).
- Anthropic will **delete all customer data within 30 days** of contract termination (DPA clause H.1).
- Anthropic encrypts customer data using AES-256 at rest and TLS 1.2 or higher in transit (DPA Schedule 2 Section E).
- All Anthropic personnel with access to customer data must authenticate via Multi-Factor Authentication (DPA Schedule 2 Section B.4).
- Anthropic engages qualified external assessors for annual penetration testing (DPA Schedule 2 Section G.2). Summary reports are available to customers on request.
- International data transfers are protected by Standard Contractual Clauses Module Two (controller to processor), with the UK Addendum and Swiss Addendum incorporated where applicable (DPA Schedule 3).
- Anthropic maintains SOC 2 Type II certification and ISO/IEC 27001 certification. Anthropic's full Trust Center, including current certifications, sub-processor list, and the public-facing DPA, is available at trust.anthropic.com.
- Edsthetic holds annual audit rights over Anthropic's compliance with the DPA (DPA clause F.2).

10.4 What schools should know about AI-assisted feedback

Writeiq deliberately does not present AI as a substitute for teacher judgement. AI-produced scores are always presented as a recommendation that the teacher can accept, adjust, or reject. Every teacher adjustment is recorded as a calibration data point, which feeds back into the model's accuracy over time. This is consistent with the Department of Education's guidance that AI tools in schools should support but not replace teacher professional judgement.

Writeiq's calibration target is 75 to 80 per cent exact-band agreement with teacher judgement, and 95 per cent or better within-one-band agreement. These targets are set deliberately above the level of human inter-rater reliability typically observed in writing assessment research.

11. Sub-processors

Edsthetic uses a small number of contracted sub-processors to deliver Writeiq. Every sub-processor is bound by a written agreement that includes confidentiality, security, and data handling obligations. The complete current list is set out below.

Sub-processor	Role	Hosting and certifications
---------------	------	----------------------------

Supabase, Inc.	Managed PostgreSQL database (where customer data lives) and authentication infrastructure. Data residency in Sydney AU.	Sydney AU (data) San Francisco (entity) SOC 2 Type II HIPAA-eligible ISO 27001 (via AWS) DPA with SCCs
Amazon Web Services (Amazon Bedrock)	Claude models used for AI-assisted feedback, scoring support and handwriting transcription, operated by AWS inside the Australian boundary. No training on customer content; prompts and completions are not stored; the model provider does not receive the content. Replaced Anthropic, PBC (United States) on 25 July 2026.	Australia Sydney ap-southeast-2 Melbourne ap-southeast-4 SOC 2 Type II ISO/IEC 27001 IRAP-assessed AWS DPA
Microsoft (Azure AI Document Intelligence)	Handwriting layout extraction for the optional Vision feature: reads a scanned page and returns lines, words, confidence and position so a teacher can check the transcript against the original before marking. Produces no scores or feedback. Scanned work only, never typed submissions.	Australia Azure australiaeast SOC 2 Type II ISO/IEC 27001 IRAP-assessed Microsoft Online Services DPA
Cloudflare, Inc.	Edge network: WAF, DDoS protection, bot management, TLS termination.	Global edge SOC 2 Type II ISO/IEC 27001 Sydney POP
Amazon Web Services (SES)	Transactional email delivery for invitations and notifications. Edsthetic is the sender; SES is the carrier only. No submission content. No student PII in message bodies.	Sydney AU (ap-southeast-2) ISO/IEC 27001 SOC 2 Type II 30-day bounce/complaint retention
Sentry (Functional Software, Inc.)	Error monitoring with PII scrubbing. Receives stack traces and sanitised context, not customer content.	US/EU SOC 2 Type II Privacy Shield successor frameworks
PostHog Inc.	Product usage analytics. Receives event names and timing, not student writing or feedback.	US SOC 2 Type II GDPR data processing terms
Netlify, Inc.	Static asset and serverless function hosting (the marketing site and API edge functions).	Global edge SOC 2 Type II
Stripe, Inc. — only when billing is active	Payment processing for paid (billed) deployments. No stored school, staff, or student data; billing-contact and payment details only. Not used in pilot or unbilled deployments.	United States PCI DSS Level 1 SOC 2 Type II

Edsthetic notifies schools at least thirty days in advance of any change to this sub-processor list. The current list is also published at edsthetic.com.au/legal/sub-processors.

12. Monitoring and analytics

Writeiq uses two operational monitoring tools: Sentry for error tracking, and PostHog for product usage analytics. Both are configured with privacy controls that prevent student writing, names, and other personal information from being collected or transmitted.

12.1 Sentry (error monitoring)

When something goes wrong inside Writeiq, Sentry receives a technical report describing where the error occurred so that Edsthetic engineers can investigate and fix it. The privacy controls applied to all Sentry traffic are:

- **Textarea contents are masked.** The contents of student writing fields, marking notes, and any other free-text input are replaced with asterisks before any error data is sent.
- **Password and PIN inputs are masked at the source** and never transmitted, even in their masked form.
- **URL query strings are stripped** before any error data leaves the browser. Class codes and other URL parameters are removed.
- **Network request bodies are excluded from error breadcrumbs.** Sentry sees only the URL and the HTTP status code, not the data sent or received.
- Trace sampling on the Writeiq application surface is set to **ten per cent**, meaning Sentry receives one in ten requests' performance data from school users, not all of them. Edsthetic's internal administrative tooling uses a higher sampling rate (twenty per cent) for diagnostic coverage; this surface is not customer-facing and is operated only by Edsthetic personnel.

12.2 PostHog (product usage analytics)

PostHog records anonymised events such as 'a teacher opened the marking screen' or 'a school admin generated a report'. PostHog is used to understand which features schools rely on most so the product can be improved. PostHog does not receive student writing, student names, marking comments, or any free-text content. PostHog receives only the names of events, timestamps, and aggregated context such as the user's role and school identifier.

13. Data retention, deletion and portability

13.1 During the contract

While a school's licence is active, Writeiq retains writing submissions and assessment data so that the school can maintain longitudinal records, run cohort analytics, and produce end-of-year reports. There is no automatic time-based deletion during the active contract period; the school controls its own retention policy.

Schools can delete individual student records, individual writing submissions, or whole class records at any time through the school administrator interface. Deletion is irreversible and propagates immediately to all backups within the standard backup-retention window.

For inbound bulk-import files (CSV uploads and OneRoster ZIP bundles), there is no server-side artefact to retain or delete: as described in Section 7.5, the raw file is parsed entirely in the administrator's browser and never transmitted to Edsthetic's servers. The imported row data is subject to the deletion rules above.

13.2 At end of contract

On termination of the licence, the school can either:

- Request a complete export of school data in CSV format (student records, submissions, feedback, and analytics summaries) within fourteen days of contract end, at no cost.

- Request immediate deletion of all school data from production systems. Backups containing the data are retained for thirty days (the standard backup retention window) and then permanently deleted.

If neither option is selected, the default is deletion. School data is retained for ninety days post-termination to permit re-engagement, and then permanently deleted.

13.3 Backups

Supabase performs automated daily backups of the Writeiq database, retained for thirty days. Point-in-time recovery is available for the last seven days at five-minute granularity. All backups are stored in the Sydney AU region, encrypted with AES-256, and never replicated outside Australia.

14. Incident response and breach notification

Edsthetic maintains a documented incident response procedure covering detection, containment, eradication, recovery, post-incident review, and notification. This procedure is integrated with the contractual obligations Edsthetic holds against its sub-processors.

The notification chain in a nutshell

- Supabase commits, under its DPA with Edsthetic, to notify Edsthetic of any Security Incident within **48 hours** of becoming aware of it.
- AWS commits, under the AWS Data Processing Addendum, to notify Edsthetic of a Security Incident **without undue delay** after becoming aware of it. (Until 25 July 2026, when model processing ran on the Anthropic API, Anthropic's DPA carried a 48-hour commitment.)
- Edsthetic, in turn, commits to schools to notify any school whose data is affected by a confirmed security incident within **72 hours** of confirmation. The additional 24-hour buffer allows Edsthetic to investigate scope and assemble accurate information for the school's response.

Edsthetic's commitments to schools in the event of a security incident

- Schools whose data is affected by a confirmed security incident will be notified within seventy-two hours of confirmation.
- In the case of a notifiable data breach as defined under the Privacy Act 1988 (Cth), Edsthetic will comply with all obligations under the Notifiable Data Breaches scheme, including notifying the Office of the Australian Information Commissioner.
- Schools will be provided with a written incident report including the nature of the incident, the data affected, the remediation steps taken, and the steps the school can take to protect its users.
- Edsthetic will cooperate with any state Department of Education or other regulator in the investigation of any incident.

Reporting an incident

If a school suspects a security incident or privacy breach involving Writeiq, please contact security@edsthetic.com.au. We acknowledge security reports within four working hours during Australian business hours, and the next working day for reports received outside business hours.

15. Security testing and assurance roadmap

Edsthetic's security testing posture is set out below. Items marked 'in place' are operating now. Items marked with a target date are scheduled and on the published roadmap.

Assurance	What it is	Status / Target
Internal continuous testing	Automated smoke tests on every code deployment (4,000+ checks). Pre-deployment Vite build pipeline with secret-scan gate.	In place
Real-browser regression testing	Playwright-driven Chromium harness that exercises real DOM events (clicks, navigation, form fills) against the live build. Catches a class of bug that source-level testing cannot — for example, CSS selectors that look correct in source but do not match the actual DOM tree, or window-exported functions that exist as bundle-scope variables but are missing from the click delegator's lookup path.	In place. Login flow, navigation hiding, and security boundary visibility covered. Expanding with every release.
Sub-processor compliance	All major sub-processors hold SOC 2 Type II certification (Supabase, AWS, Microsoft, Cloudflare, Sentry, PostHog, Netlify). AWS Sydney and Azure Australia East are additionally IRAP-assessed.	In place
OWASP ZAP passive manual exploration	A passive manual exploration of the live service using the OWASP Zed Attack Proxy. This was not an active penetration test. No High-risk issues were identified; SRI hardening and app-host cookie scoping were confirmed closed on the 24 May 2026 passive re-scan.	Completed. School-facing summary on request. An active ZAP DAST of staging runs before each commercial deployment and at least quarterly thereafter.
ST4S Readiness Check	Self-assessment submission to the Safer Technologies for Schools program operated by Education Services Australia.	Term 3 2026 (submission). ST4S badge target: mid-2027.
External penetration test	Manual third-party offensive security assessment by certified security professionals (CREST or equivalent) covering web application, API, authentication, and authorisation logic. Distinct from automated DAST scans.	2027
SOC 2 Type II	Independent audit of Edsthetic's own security controls (in addition to the existing certifications held by sub-processors).	2028

Edsthetic's current security testing posture is broadly equivalent to that of comparable vendors operating without an ST4S badge or SOC 2 certification. The roadmap above sets out the deliberate sequence of independent assurance milestones that will close the gap to vendors with full third-party certification, in priority order.

16. Compliance and legal posture

Australian Privacy Principles (APPs)

Edsthetic complies with the Australian Privacy Principles set out in Schedule 1 of the Privacy Act 1988 (Cth). This includes obligations relating to open and transparent management of personal information (APP 1), collection of solicited personal information (APP 3), use and disclosure of personal information (APP 6), security of personal information (APP 11), and access and correction (APPs 12 and 13).

Victorian Information Privacy Principles

Where Edsthetic holds personal information about Victorian residents (including Victorian school students and staff), the Victorian Information Privacy Principles in the Privacy and Data Protection Act 2014 (Vic) also apply. Edsthetic's data handling is designed to satisfy both the APPs and the Victorian IPPs concurrently, which in practice means meeting the higher standard of the two on every control.

Notifiable Data Breaches scheme

Edsthetic is bound by the Notifiable Data Breaches scheme under Part IIIC of the Privacy Act 1988 (Cth). In the event of an eligible data breach affecting school data, the OAIC will be notified within the timeframes required by the scheme, and affected schools will be notified directly within seventy-two hours of breach confirmation.

Data sovereignty

Customer data is stored exclusively in Australia. No customer data is replicated, mirrored, or backed up to any non-Australian location. Customer data is processed outside Australia only for the limited purpose of generating AI-assisted feedback (which is performed on Amazon Bedrock inside the Australian boundary), under the Data Processing Agreement described in Section 10.

Subject access and correction

A parent, student, or staff member who wishes to access or correct personal information held in Writeiq about themselves or (in the case of a parent) their child, should contact the school in the first instance. The school administrator can fulfil access and correction requests directly through the Writeiq interface. If a school requires Edsthetic's assistance with a subject access request, the school can email privacy@edsthetic.com.au.

17. Quick reference: PIA mapping

The following table maps the most common Privacy Impact Assessment fields to the answers your school will need. Each entry corresponds to a section of this document where the underlying detail can be found.

PIA Field	Answer / Reference
Software name	Writeiq
Vendor	Edsthetic, ABN 70 939 441 240
Vendor jurisdiction	Australia (Federal and Victorian state law)
Software URL	https://app.writeiq.com.au
Marketing URL	https://writeiq.com.au
Hosting location	Sydney, Australia (AWS ap-southeast-2)
Legal jurisdiction over data	Australian Commonwealth and Victorian state law
Data centre operator	Amazon Web Services (Sydney). ISO 27001 certified.
Database hosting provider	Supabase, Inc. (San Francisco, US-incorporated). Data hosted in Sydney AU under data residency commitment. SOC 2 Type II certified. DPA with SCCs in place.
Encryption in transit	TLS 1.2 or higher with modern ciphersuites

Encryption at rest	AES-256 with FIPS 140-2 compliant HSMs for key management
Authentication (staff)	Per-user accounts. Email + password OR Google/Microsoft SSO. TOTP MFA in place (optional for teachers, required for school admins). Passwords handled by Supabase Auth.
Authentication (students)	No email account required. Three paths: Class Links (signed URL per class, recommended); Student Access Code (school-set code, rotated by admin); Student SSO (opt-in only). public.students table has no authentication fields. See Section 7.2.
Authorisation model	Role-based access (Admin / Leader / Teacher / Student). Row-Level Security at the database layer. SECURITY DEFINER functions on all data access.
Account provisioning	Per-user invitations via SES (Sydney). Bulk CSV import + OneRoster 1.2 ZIP for classes, staff, students. Both paths admin-gated and audit-logged. Inbound files parsed entirely client-side; never transmitted to Edsthetic servers. See Section 7.5.
Audit logging	All sign-in events, admin actions, and bulk-import commits logged. Retained 12 months minimum.
AI processing	Claude models on Amazon Bedrock, Australian boundary (Sydney ap-southeast-2 / Melbourne ap-southeast-4) since 25 July 2026. AWS DPA + Amazon Bedrock service terms: no training on customer content, prompts and completions not stored, content not shared with the model provider, Security Incident notification without undue delay, SOC 2 Type II + ISO 27001 + IRAP. Typed submissions: only writing text + rubric transmitted; no student names, IDs, or school identifiers. Handwritten scans: image transmitted as scanned (any handwritten name visible); school-side UID workflow available; automated name redaction in trial for Term 3 2026 (see Section 10.2). Before 25 July 2026 this ran on the Anthropic Claude API in the United States under Anthropic's DPA effective 24 Feb 2025 (see Section 10.3.1).
Sub-processors	Supabase, Amazon Web Services (Bedrock + SES), Microsoft (Azure AI Document Intelligence, Australia East), Cloudflare, Sentry, PostHog, Netlify, plus Stripe when billing is active (full list with certifications: Section 11). Signed Supabase DPA and TIA available on request.
Cross-border data transfer for storage	Primary customer data hosted in Sydney AU. Operational data (logs, diagnostics, support records) may be processed by sub-processors in the US under SCCs and EU-US Data Privacy Framework where applicable.
Cross-border data transfer for processing	None for student writing. AI-assisted feedback, scoring support and transcription run in Australia (Amazon Bedrock, Sydney / Melbourne) since 25 July 2026; handwriting layout extraction runs in Azure Australia East. Remaining cross-border processing is operational telemetry only (Sentry, PostHog), carrying no student writing or names. Before 25 July 2026, AI-assisted feedback ran in the US (Anthropic) under written DPA with a no-training clause, with no student identifiers transmitted.
Data retention during contract	School-controlled. Default: retain until school deletes.
Data retention at contract end	Default 90 days post-termination then permanent deletion. Earlier deletion on request. CSV export available on request.
Backup retention	30 days, encrypted, in Sydney AU.
Notifiable Data Breaches scheme	Bound under the Privacy Act 1988 (Cth). 72-hour breach notification commitment to affected schools.
ST4S badge	Readiness Check submission Term 3 2026. Badge target mid-2027.

OWASP ZAP passive manual exploration	Completed; not an active penetration test; no High-risk findings. SRI and app-host cookie scoping confirmed closed on the 24 May 2026 re-scan. Active DAST of staging before each commercial deployment and at least quarterly.
Real-browser regression testing	In place. Playwright/Chromium harness exercising real click events, login flow, navigation hiding, and security boundary visibility.
External pentest	Scheduled 2027 (manual, third-party CREST-certified or equivalent).
SOC 2 Type II for Edsthetic	Targeted 2028 (sub-processors already certified).
Security incidents and responsible disclosure	security@edsthetic.com.au
Access, correction and deletion requests	privacy@edsthetic.com.au
Privacy / PIA support	legal@edsthetic.com.au

18. Glossary

Term	Plain-language definition
AES-256	The Advanced Encryption Standard with a 256-bit key. Used by the Australian Government for protected information. The standard is considered unbreakable by current computing capabilities.
API	Application Programming Interface. The technical mechanism by which one piece of software talks to another. When Writeiq sends a piece of writing for AI-assisted feedback and analysis, it does so via the Amazon Bedrock API.
AWS	Amazon Web Services. The cloud computing provider operating the Sydney data centres where Writeiq's data physically resides. Holds ISO/IEC 27001 certification for the Sydney region.
Class Link	A signed URL minted by a school administrator for a specific class. Students click the link to enter Writeiq directly. The link itself is the credential — no separate student account is required. The recommended student-access path; see Section 7.2.
Cloudflare	A network service that sits between the public internet and Writeiq's servers, providing firewalling, DDoS protection, and bot management. Protects more than twenty per cent of all websites globally.
CSRF	Cross-Site Request Forgery. A type of attack where a malicious site tricks a user's browser into making a request to another site on which the user is authenticated. Writeiq mitigates CSRF using HttpOnly Secure SameSite=Strict cookies and a double-submit token pattern.
DDoS	Distributed Denial of Service. A type of attack where many computers send traffic to a website with the goal of overwhelming it. Cloudflare absorbs and filters DDoS traffic before it reaches Writeiq's servers.
DPA	Data Processing Agreement. A written contract between a data controller (such as Edsthetic) and a data processor (such as Anthropic) that sets out how customer data will be handled.
HMAC-SHA256	A cryptographic technique used to verify that a message has not been tampered with. Used to sign Writeiq's authentication tokens so that an attacker cannot forge a valid login.
HTTPS	Hypertext Transfer Protocol Secure. The encrypted version of HTTP. The lock icon in a browser address bar indicates that HTTPS is in use. Writeiq uses HTTPS for every connection.
ISO/IEC 27001	An international standard for information security management. AWS Sydney holds this certification. Anthropic, Cloudflare, and Sentry also hold it.
JWT	JSON Web Token. A short-lived, cryptographically signed token used to confirm a user's identity to Writeiq's server. JWTs in Writeiq are delivered as HttpOnly cookies and never written to localStorage or sessionStorage on the user's device.
MFA	Multi-Factor Authentication. A second confirmation step in addition to a password (commonly a six-digit code from a phone authenticator app such as Google Authenticator, Microsoft Authenticator, or Authy). Available for all staff users; required for school administrators. Implemented using RFC 6238 Time-based One-Time Password (TOTP) with AES-GCM-encrypted secrets stored in Edsthetic's database.
OAuth 2.0	An industry-standard protocol for delegated authentication. Used when staff sign in via Google or Microsoft SSO. The school's identity provider remains the source of truth; Writeiq never sees the user's Google or Microsoft password.
OneRoster	An IMS Global standard CSV bundle format for exchanging school management data (classes, users, enrollments) between systems. Compass, Edval, Sentral, Edumate, and most other Australian school management systems can export OneRoster 1.2 bundles. Writeiq accepts these bundles for bulk onboarding; see Section 7.5.

PBKDF2	Password-Based Key Derivation Function 2. A cryptographic key-stretching technique. In Writeiq it hashes TOTP recovery codes (600,000 iterations) and derives the AES-GCM key that encrypts TOTP secrets. Staff passwords are handled by Supabase Auth, not by Edsthetic.
Playwright	An open-source browser automation framework. Writeiq uses Playwright to drive a headless Chromium browser through real user flows (clicks, form fills, navigation) as part of its continuous test suite. Catches a class of bug that source-level testing cannot. See Section 15.
PostgreSQL	An open-source database widely used by major Australian and international organisations. The underlying database technology used by Writeiq.
Row-Level Security (RLS)	A PostgreSQL feature that filters database query results so that a user can only see rows they are authorised to see. Used in Writeiq to ensure one school can never see another school's data.
SES	Amazon Simple Email Service. The transactional email service used by Edsthetic to deliver invitation claim links and account notifications to staff. Runs in the AWS Sydney region. SES carries the email; Edsthetic is the sender.
SOC 2 Type II	An independent audit standard verifying a vendor's controls over security, availability, processing integrity, confidentiality, and privacy over a period of time (typically twelve months). Held by all of Writeiq's major sub-processors.
SSO	Single Sign-On. The ability to sign into Writeiq using an existing Google or Microsoft account, without creating a new password.
ST4S	Safer Technologies for Schools. A national assessment program operated by Education Services Australia, evaluating the security and privacy of education software.
Supabase	A managed PostgreSQL database provider, headquartered in San Francisco. Writeiq uses Supabase's Sydney AU region under a data residency commitment that keeps customer data in Australia.
TLS 1.2 or higher	Transport Layer Security versions 1.2 and 1.3. TLS is the current internet standard for encrypted connections between a browser and a website. The same protocol used by every major Australian bank for online banking. Edsthetic, Supabase, and Anthropic all support TLS 1.2 with modern ciphersuites at minimum.
TOTP	Time-based One-Time Password. The MFA mechanism Writeiq uses, defined in RFC 6238. Compatible with Google Authenticator, Microsoft Authenticator, Authy, 1Password, and any other authenticator app that follows the standard.
WAF	Web Application Firewall. A security layer that filters incoming web traffic, blocking known attack patterns. Provided by Cloudflare for Writeiq.

19. Contact

If any part of this document is unclear, if your school requires additional evidence to support a specific PIA control, or if you have a privacy or security question not covered here, please contact us.

Privacy and PIA support	legal@edsthetic.com.au
Security incident reports	security@edsthetic.com.au
General enquiries	hello@edsthetic.com.au
Marketing site	https://writeiq.com.au
Application	https://app.writeiq.com.au
Sub-processor list (live)	https://edsthetic.com.au/legal/sub-processors
Privacy policy	https://edsthetic.com.au/legal/privacy

Edsthetic responds to privacy enquiries from school IT, leadership, and Privacy Officer staff within two working days, and to security incident reports within four working hours during Australian business hours.

Document control

Title	Writeiq — Security and Privacy Overview
Version	1.7
Issue date	26 July 2026
Owner	Edsthetic, ABN 70 939 441 240
Review cycle	At every major platform release, or on regulatory change, whichever comes first.
Distribution	Provided to schools considering or implementing Writeiq, and to school IT and Privacy teams on request.

Changelog from v1.4 → v1.7

v1.5 (interim, May 2026): Section 6 token storage clarification — JWT in HttpOnly cookies; no auth tokens in localStorage or sessionStorage. Section 7.2 access-code rotation wording — administrator-controlled, not auto-expiring (deliberate UX). Section 12.1 Sentry sampling scope — refers specifically to the Writeiq application surface, with internal admin tooling on a separate sampling rate. Section 18 MFA glossary entry — updated to reflect TOTP MFA in production (previously marked roadmap).

v1.6 (12 May 2026): Section 7.2 expanded into a PIA-critical section making student access architecture explicit (no email required; three access paths; `public.students` has no authentication fields). New Section 7.5 documents account provisioning end to end: per-user invitations via SES, bulk CSV import for classes/staff/students, and OneRoster 1.2 ZIP pre-processor. The client-side parsing security principle (inbound files never reach Edsthetic servers in raw form) is documented explicitly. Section 6 encryption table adds rows for browser storage and inbound CSV/ZIP files. Section 11 sub-processor table adds AWS SES (Sydney) for transactional email. Section 15 adds Playwright real-browser regression testing as an in-place control. Section 18 glossary adds CSRF, Class Link, OneRoster, Playwright, SES, and TOTP entries; corrects TLS entry. Section 17 PIA mapping table extended with student authentication, account provisioning, and real-browser regression testing rows. References to TLS 1.3 corrected throughout to TLS 1.2 or higher.

v1.7 (26 July 2026) - Australian residency for model processing. On 25 July 2026 the AI-assisted feedback, scoring-support and handwriting-transcription step moved from the Anthropic API in the United States to Claude models running on Amazon Bedrock inside the Australian boundary (AWS Sydney `ap-southeast-2` and Melbourne `ap-southeast-4`). Storage was already Australian; with this change no student writing or student name leaves Australia at any stage. Section 10 is retitled and its contractual basis (10.3) is rewritten to the AWS Data Processing Addendum and Amazon Bedrock service terms, with the previous Anthropic position kept as historical sub-section 10.3.1 because it governs work marked before the cutover. Section 5.1 cross-border row updated. Section 11 replaces the Anthropic, PBC row with Amazon Web Services (Amazon Bedrock) and adds Microsoft (Azure AI Document Intelligence, Australia East) for the optional Vision handwriting-extraction path. Residency is enforced in code rather than by configuration alone: a model with no Australian route is refused and a request that cannot be served onshore fails or queues, so there is no automatic fallback to an overseas region. The remaining processing outside Australia is operational telemetry (Sentry, PostHog), which carries no student writing or names.