FOR SCHOOLS & DISTRICTS

Evident School Procurement Packet

This packet is a self-serve starting point for school leaders, privacy officers, IT reviewers, and procurement teams evaluating Evident. It summarizes current product practices and links to the public trust surfaces that should be reviewed before a pilot or purchase.

CONTENTS

Security overview
Data privacy summary
Student privacy commitments
DPA / NDPA information
Subprocessor list
Data retention and deletion
FERPA-conscious workflow explanation
AI usage statement
Accessibility statement
Implementation FAQ
Rostering and provisioning options
Support and contact path
Review links

Security overview

Controls designed to protect student-support records.

Evident uses Supabase-hosted PostgreSQL with Row Level Security policies to keep users and organizations scoped to the records they are authorized to access.

Application access is authenticated, role-aware, and designed around teacher, school admin, and organization membership boundaries.

Data is encrypted in transit with HTTPS/TLS and encrypted at rest by the hosting and database providers.

Data privacy summary

How student-support data is collected, used, and controlled.

Evident stores student display names, goals, daily logs, evidence notes, family-visible summaries, parent portal interactions, and account metadata needed to provide the service.

Teachers and school admins control what becomes family-visible. Staff-only notes are not shown to families unless a user explicitly publishes family-visible content.

Evident is designed for data minimization and recommends using student display names instead of unnecessary sensitive identifiers.

Student privacy commitments

Twelve public promises, each tied to a control.

Evident publishes twelve public commitments about student personal information at evidentk12.com/student-privacy: collect only what the service needs; never sell it; never use it for advertising; build no profile beyond the authorized purpose; no material handling changes without 30 days notice to the school; keep nothing longer than needed; use it only for authorized purposes; disclose clearly what is collected and who touches it; support access and correction through the school; maintain a security program; hold sub-processors to the same terms; and bind any successor.

Each commitment is paired on that page with the product or contract control that makes it true. The industry Student Privacy Pledge these mirror was retired in April 2025, so Evident makes them directly as public representations rather than claiming a signatory status that no longer exists.

DPA / NDPA information

Contracting path for school privacy review.

Evident provides DPA/NDPA documentation for schools and districts evaluating or using the product.

District-specific terms can be reviewed through the privacy contact path when a standard agreement does not satisfy local requirements.

The DPA page provides DPA information, subprocessor details, and the request path for agreement documentation.

For districts that use the Student Data Privacy Consortium's National Data Privacy Agreement (NDPA v2.2), Evident keeps its provider exhibits pre-completed (products and services, schedule of student data, general offer of privacy terms, cybersecurity framework) so a district's copy can be returned promptly; Evident signs the standard clauses unchanged and offers a 24-hour breach notice in place of the standard 72.

Subprocessor list

Core vendors used to host, operate, bill, email, monitor, and protect the service.

Vercel: hosting and application compute.

Supabase: database, authentication, and storage-backed application services.

Stripe: payment processing and billing portal.

Resend: transactional email delivery.

Sentry: error monitoring.

Upstash: rate limiting infrastructure.

PostHog: privacy-conscious product analytics (no student names or note content).

OpenAI: AI-assisted translation, note polish, public-site help and the optional Ask Evident research companion, only where explicitly invoked (US deployment). Ask Evident sends user-reviewed general questions and conversation context, without attaching roster or student records; optional saved history is private and deletable.

Anthropic: AI-drafted, teacher-reviewed IEP progress narratives, only where the feature is explicitly invoked (US deployment).

Mistral AI: translation on the EU deployment, with student names redacted before any request.

Data retention and deletion

How data export, deletion, and disposition requests are handled.

Teachers and authorized admins can view, export and delete student and account data themselves in the product (JSON export on every plan; CSV and PDF reports on school and Pro plans), and an organization owner can export the whole organization's data in one action. No request to Evident is needed.

Audit logs are insert-only. IP addresses and browser details are removed from entries after 90 days, the entries themselves are deleted after 24 months, and all of them are removed with the account under the standard disposition timeline.

School or district disposition requests should be sent through the privacy contact path so scope, timing, and verification can be confirmed.

Retention behavior should be reviewed against the signed agreement for each school or district.

FERPA-conscious workflow explanation

Product controls that support school FERPA obligations.

Evident is designed to support FERPA-conscious workflows through role-based access, staff-only notes, explicit family visibility controls, audit logs, export/delete workflows, and DPA support.

Schools remain responsible for their own FERPA determinations, directory information policies, parent rights processes, and internal staff training.

AI usage statement

Where AI may be used and how to review it.

Evident uses AI-supported functionality only where a product feature explicitly invokes assistance: translation, note polish, AI-drafted IEP progress narratives, chart drafts from a teacher's description of what a student is working on, and chart themes from a single teacher-typed keyword. Translation, note polish, narratives and chart drafts mask the student's name before sending text; theme requests carry no student data. School admins can disable AI note polish and AI progress narratives for their organization; those controls do not disable translation. Review free text before requesting assistance because it may contain other identifying details.

AI-assisted outputs must be reviewed by an educator before being shared with families or used in formal documentation; progress narratives cannot be exported until a teacher marks them reviewed.

Evident should not be described as making automated eligibility, discipline, placement, or service decisions.

Accessibility statement

Current accessibility target and readiness path.

Evident targets accessible, keyboard-friendly workflows for educators and families and maintains an accessibility guide for core patterns.

A public accessibility readiness statement documents current audit scope, known gaps, and the path toward VPAT/ACR readiness.

Formal VPAT/ACR completion should not be claimed until the readiness work and review are complete.

Implementation FAQ

How a school can pilot and roll out Evident.

Most schools can start with a small Support Team or school plan using invitations and CSV import before deeper rostering integrations are required.

School admins can invite staff, manage seats, and review school-level usage from the admin dashboard.

Pilot scope should define participating staff, student-support workflows, review dates, and success metrics before launch.

Rostering and provisioning options

Current and future paths for getting staff and students into Evident.

Current pilot-friendly options include staff invitations and CSV student import.

Clever, ClassLink, and OneRoster readiness should be evaluated through a separate integration audit before being promised as a production rollout path.

Support and contact path

Where schools send procurement, privacy, security, and implementation questions.

School purchasing and pilot questions can be sent to schools@evidentk12.com.

Privacy and DPA questions can be sent through the privacy contact path.

Security review questions can be sent through the security contact path.

Review links

The public pages this packet summarizes, for a reviewer to read in full.

Security	https://evidentk12.com/security
Compliance	https://evidentk12.com/compliance
DPA / NDPA	https://evidentk12.com/privacy/dpa
Student privacy commitments	https://evidentk12.com/student-privacy
Privacy & security plan (NY Ed Law 2-d)	https://evidentk12.com/privacy-security
Accessibility	https://evidentk12.com/accessibility
School plans	https://evidentk12.com/school-signup