FOR NEW YORK EDUCATIONAL AGENCIES

Evident Data Privacy and Security Plan

New York Education Law §2-d and 8 NYCRR Part 121

This document is the Data Privacy and Security Plan that 8 NYCRR §121.6 requires of a third-party contractor, and the supplemental information that §121.3(c) requires the educational agency to attach to its Parents' Bill of Rights for Data Privacy and Security. The educational agency may attach it to its agreement with Evident as written, post the supplemental information with its Bill of Rights, or ask Evident to complete the agency's own template; the commitments are the same either way.

CONTRACTOR	5minMindful LLC, operating the Evident service (https://evidentk12.com), 2803 Philadelphia Pike, Suite B #569, Claymont, DE 19703.
DESIGNATED REPRESENTATIVE	Ben Stone, Founder, privacy@evidentk12.com.
SECURITY NOTICES	security@evidentk12.com
PUBLISHED AT	https://evidentk12.com/privacy-security

CONTENTS

Supplemental information for the Parents' Bill of Rights for Data Privacy and Security

The exclusive purposes for which the student data will be used

How Evident ensures that subcontractors, persons or entities with access to the data abide by the same data protection and security requirements

When the agreement expires and what happens to the student data when it does

If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data

Where the student data will be stored, and the security protections taken to ensure it will be protected

How the data will be protected using encryption while in motion and at rest

Data Privacy and Security Plan

Scope, parties and the law this plan follows

Administrative, operational and technical safeguards

How Evident meets each contractor obligation in §2-d and §121.9

Training of people with access to student data

Subcontractors and how they are managed

Data security and privacy incidents

Return, transition and deletion when the agreement ends

Signature, review cycle and changes

Signature

Supplemental information for the Parents' Bill of Rights for Data Privacy and Security

Education Law §2-d(3)(c); 8 NYCRR §121.3(c). To be attached to the educational agency's Parents' Bill of Rights for Data Privacy and Security for this agreement.

ITEM 1 OF 6

The exclusive purposes for which the student data will be used

Evident uses student data for one purpose: to provide the educational agency's staff with the Evident service they contracted for. That service lets teachers, learning-support staff, counselors and school administrators record goal-setting and progress data for individual students, keep dated observation notes, maintain support-plan goals and data points, record behavior incidents and intervention plans, share plain-language updates with the student's family, and assemble progress reports and evidence packets for meetings.

Evident does not use student data for any other purpose. It is never sold, never used for advertising or marketing of any kind, never used to build a profile of a student for a purpose other than the educational work the agency authorized, and never used to train an artificial-intelligence model. Where a teacher asks for optional AI assistance, the student's name is removed or replaced with a placeholder before any text leaves Evident, the provider is barred by contract from training on it, and the draft is reviewed by the teacher before it can be used.

ITEM 2 OF 6

How Evident ensures that subcontractors, persons or entities with access to the data abide by the same data protection and security requirements

Evident has no employees. The founder is the only person with access to production systems. Before any other person is granted access they will complete the training described in this plan and sign a written confidentiality agreement that binds them to the requirements of Education Law §2-d, Part 121 and the agreement with the educational agency.

Every subcontractor (sub-processor) that can touch student data is bound by a written data processing agreement that requires it to protect the data no less strictly than Evident does, to use it only to provide its service to Evident, never to sell it or use it for advertising, to notify Evident of a breach, and to delete it when the service ends. The current list, with each vendor's function and processing location, is published at evidentk12.com/security and in this plan, and the educational agency receives at least 30 days' written notice before any new subcontractor touches its data, with the right to object.

ITEM 3 OF 6

When the agreement expires and what happens to the student data when it does

The agreement runs for the term stated in the educational agency's contract or purchase order with Evident. When it expires or is terminated, Evident returns the agency's data in machine-readable form (an organization-level export in JSON and CSV with a manifest describing every table, plus the attachment files) if the agency asks for it, and deletes every student record the agency holds with Evident from production and file storage within 60 days, or sooner on request. Encrypted backups roll off within 30 days of deletion. Evident sends the agency written certification of the deletion naming the date and the backup horizon.

The agency's own administrators can also delete students, schools or the whole organization, and the organization's owner can export all of its data, at any time during the agreement without asking Evident.

ITEM 4 OF 6

If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data

Student data in Evident is entered by the educational agency's own staff, and those staff can view, correct and delete any record directly in the product at any time. A parent or eligible student who believes a record is inaccurate should raise it with the educational agency under the agency's own procedure for challenging the accuracy of student data; the agency's staff can make the correction in Evident immediately.

If the agency needs Evident's help to locate, correct or delete a record, Evident does so within 30 days of the agency's written request. Evident does not accept correction requests directly from parents, because the agency holds the record and decides what it should say; a parent who contacts Evident is referred to the agency, and Evident tells the agency it happened.

ITEM 5 OF 6

Where the student data will be stored, and the security protections taken to ensure it will be protected

All student data under the agreement is stored and processed in the United States. The database, authentication service and file storage run on Supabase in Amazon Web Services data centers in the United States; the application runs on Vercel in the United States. No student data from a New York educational agency is stored in, or transferred to, Evident's separate European deployment or any location outside the United States.

The data is protected by encryption in transit and at rest, row-level security enforced by the database on every table that holds student data, role-based access with least privilege, multi-factor authentication, an insert-only audit log the agency's administrators can read, automated tests that exercise tenant isolation on every change before it reaches production, continuous security monitoring, an annual internal security assessment and an annual internal penetration test. The safeguards are described in full in the plan below and are organized around the NIST Cybersecurity Framework.

ITEM 6 OF 6

How the data will be protected using encryption while in motion and at rest

In motion: every connection to Evident, including from the browser extension and the iOS app, and every connection between Evident and a subcontractor, is encrypted with TLS 1.2 or newer; TLS 1.3 is used wherever the client supports it. Plain HTTP requests are redirected to HTTPS, and browsers are instructed to use only HTTPS for evidentk12.com (HTTP Strict Transport Security).

At rest: the database, its daily backups, and every file attachment are encrypted with AES-256. Integration credentials held on a staff member's behalf are additionally encrypted at the application layer with a key kept outside the database. This meets the standard in New York State Technology Law §208: the data is rendered unusable, unreadable and indecipherable without the key, and the keys are held by the hosting providers and Evident, never alongside the data.

Data Privacy and Security Plan

8 NYCRR §121.6(a). The sections follow the order of the regulation's required contents.

EDUCATION LAW §2-D; 8 NYCRR §121.6(A)(1)

Scope, parties and the law this plan follows

Who the contractor is, what the service does, what data it holds, and the policies and laws Evident will follow for the life of the agreement.

The contractor is 5minMindful LLC, a Delaware limited liability company based in Ithaca, New York, which operates the Evident service at evidentk12.com. Its designated representative for this plan is Ben Stone, Founder, 2803 Philadelphia Pike, Suite B #569, Claymont, DE 19703, privacy@evidentk12.com.

Evident is a web application, with an optional browser extension and iOS companion app, in which the educational agency's staff record goal-setting and progress data, observation notes, behavior records, support-plan goals and family updates for individual students, and produce progress reports and evidence packets. Students do not have accounts. Families view only what a teacher chose to share, through a signed, revocable link, without creating an account. Student data enters Evident only by being typed, captured or uploaded by the agency's own staff; no student information system, rostering or learning-management integration is enabled unless the agency adds one by written addendum.

The student data Evident holds

- The student's name as a teacher types it (Evident asks for a first name or nickname rather than a full legal name), an optional grade level, and an optional school within the agency's organization.
- Goal and progress records: daily goal check-offs, data points such as trials, prompt levels, durations and task-step results, and the student's own self-rating on a chart where a teacher enables it.
- Behavior records: daily behavior entries, incident records (antecedent, behavior, consequence) and behavior intervention plans where entered.
- Support-plan information where a school uses those features: plan status (IEP, 504 or RTI tier), goals, accommodations and their implementation notes.
- Teacher-written observation notes and support notes, documents a teacher adds to a student's record, screenshots or photos of student work a teacher captures, family-facing summaries and their translations, and teacher-reviewed AI-drafted progress narratives.
- Family-link activity: view timestamps, a guardian's typed or drawn signature on a daily record, and any reply a family member sends back through the link.
- Staff account information: name, email address, role and organization membership of the agency's staff who use Evident.

What Evident does not collect

Evident has no field for a Social Security number, date of birth, home address, student or parent contact information, state or local student identification number, standardized test score, attendance, grades, financial information, biometric data or device location. Evident has no field for a medical diagnosis and discourages entering one in free text.

Policies and laws Evident will follow

For the life of the agreement Evident will comply with the educational agency's Data Security and Privacy Policy as adopted under §121.5, with Education Law §2-d and 8 NYCRR Part 121, with the Family Educational Rights and Privacy Act (FERPA, 20 U.S.C. §1232g and 34 CFR Part 99), with the confidentiality provisions of the Individuals with Disabilities Education Act (34 CFR §§300.610 to 300.627) where the agency's data includes special-education records, and with the Children's Online Privacy Protection Act. Evident acts as a school official with a legitimate educational interest under the agency's direct control, as FERPA allows, and will sign the agency's Parents' Bill of Rights for Data Privacy and Security together with the supplemental information in this plan.

Evident's security program is organized around the NIST Cybersecurity Framework, the standard §121.5 adopts for every educational agency's policy. Evident is not certified against ISO 27001 and holds no third-party SOC 2 report of its own; its annual assessment is structured to the SOC 2 Trust Services Criteria and is available to the agency under confidentiality on request.

8 NYCRR §121.6(A)(2); §2-D(5)(F)(5)

Administrative, operational and technical safeguards

The specific controls that protect student data, arranged by the five NIST Cybersecurity Framework functions.

Identify

- A written inventory of every data element Evident holds about students, families and staff, kept in step with the database schema and provided to the agency as the data-elements exhibit of the agreement.

- A published register of every subcontractor, with its function and processing location, reviewed whenever a vendor is added, replaced or removed.
- An annual internal security and privacy assessment with a written report, a findings log with owners and dates, and a review of every administrative account on the platform and on each provider console.
- A written incident response plan, reviewed annually and after any significant incident.

Protect

- Encryption in transit (TLS 1.2 or newer, TLS 1.3 preferred) and at rest (AES-256 for the database, its backups and all file attachments).
- Row-level security enforced by the database engine on every table that holds student data, so a request from one teacher cannot return another teacher's students even if application code is bypassed.
- Role-based access with least privilege: teacher, school administrator, organization administrator, district administrator, principal and counselor roles, per-student sharing with view-only roles, and confidential counselor notes segregated at the database layer.
- Multi-factor authentication (authenticator app with hashed single-use recovery codes) available to every account, with a deployment-level switch that requires it for administrative roles and a second switch that requires it for all staff.
- No student accounts and no student passwords. Family access only through signed, revocable links that a teacher issues and can withdraw at any time.
- The optional browser extension authenticates through an explicit user-approved authorization flow, receives its own short-lived session that an administrator can disable for the whole organization, and reads a page only when the teacher clicks capture.
- Data minimization built into the product: display names rather than full names, no fields for prohibited categories, and student names removed or replaced with placeholders before any text is sent to an AI provider.
- Secure development: every change passes an automated test suite, including database integration suites that exercise tenant isolation against a live database with row-level security enforced, before it can be deployed; dependencies are checked against published vulnerability advisories and updated; secrets are held in the hosting provider's encrypted configuration, never in source code.
- No employees or contractors hold production access. Any future grant will be role-scoped, recorded, and revoked within 24 hours of a role change or departure. Service credentials are rotated on any suspected compromise and on any personnel change.
- Audit entries lose IP address and browser details after 90 days and are deleted after 24 months; deleted notes are purged after 30 days; a deleted account is removed from backups within 30 days.

Detect

- An insert-only audit log of every student-record action (who, what, when), readable and filterable by the agency's administrators in the dashboard.
- Continuous security monitoring with alert workflows for injection attempts, anomalous bulk export, cross-tenant access attempts, brute-force sign-in and credential misuse.
- Error monitoring with personal fields scrubbed before transmission, and external uptime monitoring against a public health check.
- A published vulnerability disclosure policy with safe harbor, a machine-readable security contact at /.well-known/security.txt, and an internal penetration test of the full application at least annually (most recently June 2026, with no critical or high findings).

Respond

- The incident response plan summarized in the incidents section below: classification, containment with forensic preservation, notification to the educational agency within 24 hours of Evident becoming aware, and a post-incident review within 14 days of resolution.

Recover

- Automated daily encrypted database backups, with the ability to restore to a verified clean state; the application can be redeployed from source in minutes, and the database can be placed in read-only mode while an incident is contained.
- A written continuity and exit plan: at least 90 days' written notice before the service would ever end, a read-only period during which staff can export and print, delivery of the organization export at the start of the wind-down, and an emergency-access arrangement so that a named second person can execute the plan if the founder cannot.

EDUCATION LAW §2-D(5)(E) AND (F); 8 NYCRR §121.3(C), §121.9

How Evident meets each contractor obligation in §2-d and §121.9

Each duty the law places on a third-party contractor, and the control that meets it.

- Limit internal access to those with a legitimate educational interest. Access in Evident is granted by the agency's own administrators to their own staff, by role, and is enforced by the database. No one at Evident reads student data in the course of operating the service; the founder's production access is used for operations and support only and is reviewed at each annual assessment.
- Not use the data for any purpose other than those explicitly authorized in the agreement. Student data is used only to provide the service, as the supplemental information states. Evident does not create de-identified data sets from student data for research or product improvement; product improvement relies on pseudonymous usage analytics about how staff interact with the application, which contain no student data and are switched off on the pages families open.
- Not disclose the data to any other party without the prior written consent of the parent or eligible student, unless required by statute or court order. Evident discloses student data only to the subcontractors listed in this plan, and only as the service requires. If Evident receives a subpoena, warrant or court order for the agency's data, it notifies the agency before responding unless the law prohibits the notice, and discloses only what the order compels.
- Maintain reasonable administrative, technical and physical safeguards. The safeguards section above; physical security of the data centers is maintained by the hosting providers under their own independent third-party audits.
- Use encryption to protect the data while in motion and while at rest. As stated in the supplemental information: TLS 1.2 or newer in motion, AES-256 at rest, consistent with State Technology Law §208.
- Not sell the data, and not use or disclose it for any marketing or commercial purpose, or permit another party to do so. There is no advertising anywhere in the product, the extension or the mobile app; no advertising cookies, pixels or ad networks; no sale of data to anyone, including as part of a change of ownership except to a successor bound by the same commitments.
- Not permit the data to be used to target advertising, to amass a profile, or to track a student across services. Evident holds no student contact information, sets no cookies for students or families, and runs no cross-site tracking.
- Comply with the agency's Parents' Bill of Rights. Evident signs the agency's Bill of Rights, attaches the supplemental information above, and will provide it to the agency for posting on the agency's website as §2-d(3)(c) requires.
- Notify the agency of a breach without unreasonable delay. Within 24 hours of becoming aware, as the incidents section describes, which is well inside the seven calendar days §2-d(6)(b) allows.
- Cooperate with the agency and with law enforcement, and with the New York State Education Department's Chief Privacy Officer, in any investigation of a breach or of a complaint under §2-d. A parent or eligible student may file a complaint about a possible breach with the agency or directly with the Chief Privacy Officer; Evident answers any such inquiry fully and promptly.

8 NYCRR §121.6(A)(4), §121.7

Training of people with access to student data

Everyone who can reach student data is trained on the federal and state law that protects it before access and every year after.

Evident is operated by its founder, who is today the only officer, employee or assignee with access to student data. The founder completes a documented annual review of the federal and state laws governing the confidentiality of student data (FERPA, the IDEA confidentiality provisions, COPPA, Education Law §2-d and Part 121, and New York's breach-notification requirements) and of Evident's own incident response plan and this plan, before each annual security assessment is signed. The date of the most recent completion and the materials covered are recorded with the assessment and provided to the educational agency on request.

Before any additional officer, employee or contractor is granted access to systems that hold student data, that person completes the same training and signs a written confidentiality agreement that binds them to the requirements of §2-d, Part 121 and the agreement with the agency, and repeats the training annually while access continues. Training records are kept for the life of the agreement.

8 NYCRR §121.6(A)(5), §121.9(B)

Subcontractors and how they are managed

The companies that can touch student data on Evident's behalf, what each one does, and the contract and oversight that bind them.

Evident will use subcontractors (sub-processors) to provide the service. Each one performs a single, named function, receives only the data that function requires, and is bound by a written data processing agreement that passes through the obligations in this plan: use the data only to provide its service to Evident, protect it with safeguards no less strict than Evident's, never sell it or use it for advertising or for training a model, notify Evident of a breach so that Evident can meet its own notification clock, and delete it when the service ends. The subcontractors used for a New York educational agency's data are:

- Supabase: Database & Auth. Processing location: USA.
- Vercel: Hosting & Compute. Processing location: USA.
- Stripe: Payment Processing. Processing location: USA.
- OpenAI: AI-assisted translation, optional AI note polish, public-site help and the optional Ask Evident research companion (US deployment). Writing/translation text is redacted; free-text help and research questions are reviewed by the user for identifying details before sending, without attached roster records.. Processing location: USA.
- Anthropic: AI progress-narrative drafting for IEP progress reports, where explicitly invoked, and chart-theme generation from a teacher-typed keyword (US deployment; student names replaced with placeholders before sending, no student data in theme requests). Processing location: USA.
- Resend: Email Delivery. Processing location: USA.
- Sentry: Error Monitoring. Processing location: USA.
- Upstash: Rate Limiting (Redis). Processing location: USA.
- PostHog: First-party product analytics & session replay (masked). Processing location: USA.

Evident reviews each subcontractor's independent security attestation (for example a SOC 2 Type II report) and its data processing terms before engaging it, keeps a record of the executed agreement, and reviews the list at each annual assessment. The educational agency receives at least 30 days' written notice before any new or replacement subcontractor touches its data and may object on reasonable data-protection grounds, with the right to end the agreement and have its data returned and deleted if the objection cannot be resolved. The current list is always published at evidentk12.com/security and on the Data Processing Agreement page.

Two of the subcontractors are AI providers used only when a teacher explicitly asks for optional assistance (translation of family-facing text, note polish, drafting of a progress narrative, or a chart theme from a typed keyword). Student

names are removed or replaced with a placeholder before any text is sent, student identifiers, emails and school names are never sent, the providers are contractually barred from training on the data, every draft requires teacher review, and the agency's administrator can disable the drafting features for the whole organization.

EDUCATION LAW §2-D(6); 8 NYCRR §121.6(A)(6), §121.10

Data security and privacy incidents

How breaches and unauthorized disclosures are detected, contained and reported, and what the educational agency receives within 24 hours.

Identifying an incident

Evident's written incident response plan follows the NIST Cybersecurity Framework and NIST SP 800-61. Security alert workflows, the database audit log, authentication logs and error monitoring are correlated to determine whether an event is an incident and at what severity. A confirmed or suspected unauthorized access to, or acquisition of, student data is Severity 1 and starts the notification clock. When in doubt, Evident classifies upward, and a lower-severity event that later shows evidence of data access is reclassified the moment that evidence appears.

Containment comes before diagnosis: the affected path is isolated by revoking credentials, blocking an origin, disabling an endpoint or placing the database in read-only mode, and forensic evidence (logs, audit trails, snapshots) is preserved before any change that could alter it.

Notifying the educational agency

Evident notifies the educational agency of a breach or unauthorized release of student data in the most expedient way possible and without unreasonable delay, and in every case within 24 hours of becoming aware of it, even while the investigation continues. Education Law §2-d(6)(b) allows up to seven calendar days; Evident commits to 24 hours so that the agency keeps the rest of its own window for the notices it owes parents and the Chief Privacy Officer. The first notice goes by email with read receipt to the signatory named in the agreement, and by telephone followed by email where more than 100 students are affected, and it is updated as facts are confirmed.

- Evident's identification and a direct contact for the incident.
- The timeline: when the breach occurred, when Evident discovered it, and when it was contained.
- A plain-language description of what happened, written so the agency can forward it to parents.
- The specific student data elements affected, by reference to the data-elements exhibit of the agreement.
- The students, or the schools and classrooms, affected, or a statement that scope is still being determined and when it will be known.
- The corrective actions taken and the remediation still under way.

Parent notification, cooperation and costs

Under §2-d(6) the educational agency notifies affected parents and eligible students, and Evident supplies the plain-language description and whatever further detail the agency needs for that notice. Evident does not contact parents directly about a breach unless the agency asks it to. Where the breach is attributable to Evident's own act or omission, Evident promptly reimburses the agency for the full cost of the parent notifications the law requires. Evident cooperates with the agency, with law enforcement and with the Chief Privacy Officer to protect the integrity of any investigation, and provides the agency a redacted internal incident report (timeline, root cause, scope, remediation) within ten business days of its written request.

After the incident

After any Severity 1 or 2 incident Evident conducts a formal post-incident review: factual timeline, root cause, which controls worked and which gaps were exposed, and dated action items. Findings are folded into monitoring rules, this plan and the incident response plan within 14 days of resolution, and are listed in the next annual assessment. If the agreement is terminated because of the breach, the agency's data is returned and deleted within 60 days with written certification.

8 NYCRR §121.6(A)(7), §121.9(A)(4)

Return, transition and deletion when the agreement ends

Whether, how and when the data is returned to the agency, handed to a successor, or destroyed, at the agency's option and direction.

When the agreement expires or is terminated by either party, the educational agency chooses, and Evident does, one or more of the following:

- Return. Evident delivers the organization-level export to the agency's named contact: every table of the agency's data in JSON and CSV (students, goals, progress and behavior records, notes including confidential counselor notes, support plans, documents, the staff list, the family-link register without its live tokens, and the audit trail), the attachment files, and a manifest that lists every table with its columns, types and row counts, so the archive can be read without Evident. The organization's owner account can also run this export at any time.
- Transition to a successor contractor. The same export, in documented open formats, delivered to the agency or, at the agency's written direction, to the successor; Evident answers the successor's questions about the format for 90 days after delivery.
- Deletion. Every student record the agency holds with Evident, including attachments and derived data, is deleted from production and file storage within 60 days of expiration or termination, or sooner on request, and encrypted backups roll off within 30 days of that deletion. Evident sends the agency written certification naming the date of deletion and the date after which no backup contains the data. Deletion is a cascading delete scoped by the database's row-level security to the agency's organization, so no other agency's data is touched.

During the time between notice of termination and deletion the service stays available to the agency's staff at least read-only, so they can export and print. Staff accounts belonging to the agency are deactivated at the agency's direction, and any browser-extension or mobile sessions they hold are revoked with them. Evident keeps only what the law or its own tax and billing records require about the agency as a customer, none of which is student data.

8 NYCRR §121.6(B)

Signature, review cycle and changes

How the plan is signed, how often it is reviewed, and the notice the agency receives before anything in it changes.

This plan is version 1.0, dated 2026-10-15. Evident provides it on request as a signed document on company letterhead, together with the supplemental information for the agency's Parents' Bill of Rights and the agency's own Bill of Rights countersigned, and will complete the agency's own plan template instead where the agency requires its form. Evident reviews the plan at least annually, with the annual security assessment, and after any Severity 1 or 2 incident or significant change to its systems.

Evident will only change this plan to make a protection stronger or a description more accurate. Any change that would weaken a commitment, change how student data is used, or add a subcontractor is a material change: the educational agency receives at least 30 days' written notice before it takes effect and may end the agreement, with its data returned and deleted, instead of accepting it. The current version is always published at evidentk12.com/privacy-security, and the version an agency signed remains the one that governs its agreement until it accepts a later one.

Questions about this plan: privacy@evidentk12.com. Security notices: security@evidentk12.com.

Signature

5minMindful LLC (Evident) agrees to the commitments in this Data Privacy and Security Plan and in the supplemental information above for the educational agency's Parents' Bill of Rights for Data Privacy and Security.

Signed _____

Name and title: Ben Stone, Founder, 5minMindful LLC _____

Date _____

Educational agency _____

Agreement or purchase order _____