

# Precision Start™

## Trust & Compliance Packet

**For School IT, Legal, and Procurement Teams**

This packet contains the documentation needed to support a vendor security and compliance review of Precision Start™ by Third Eye Education Analytics LLC.

### **CONTENTS**

- Privacy Policy
- FERPA Compliance Statement
- Security Overview
- Subprocessor List
- Breach Notification Plan Summary
- Data Processing Agreement Request Information

### **ABOUT PRECISION START™**

Precision Start™ is a teacher-facing math intervention planning platform serving K-8 schools. We help teachers identify prerequisite skill gaps before a unit begins, group students by shared instructional need, and deliver matched intervention plans -- turning the first three weeks of a unit from diagnostic guesswork into Day 1 action.

## **ABOUT THIRD EYE EDUCATION ANALYTICS LLC**

Third Eye Education Analytics LLC is a Washington, DC-based education technology company founded by Andre A. Aina, a DC educator and Math Education and Policy Advocate.

## **FOR QUESTIONS OR TO REQUEST A COPY OF OUR DATA PROCESSING AGREEMENT**

Andre Aina, Principal [andre@thirdeyeanalytics.org](mailto:andre@thirdeyeanalytics.org)

## **LIVE VERSIONS OF ALL DOCUMENTS**

- [precision-start.com/privacy](https://precision-start.com/privacy)
- [precision-start.com/ferpa](https://precision-start.com/ferpa)
- [precision-start.com/security](https://precision-start.com/security)
- [precision-start.com/subprocessors](https://precision-start.com/subprocessors)

**Document version date:** August 31, 2026

## Table of Contents

---

1. **Privacy Policy** -- Data collection, processing, AI usage, and student privacy protections
2. **FERPA Compliance Statement** -- School official designation, parental rights, de-identification
3. **Security Overview** -- Infrastructure, encryption, access control, audit logging
4. **Subprocessor List** -- Third-party services, data transmission, AI training restrictions
5. **Breach Notification Plan Summary** -- Severity levels, 5-phase response, notification timelines
6. **Data Processing Agreement** -- How to request the DPA for your organization

# Privacy Policy

**Precision Start™ by Third Eye Education Analytics LLC Effective: March 2026 | Updated: July 15, 2026**

## 1. Who We Are

---

Third Eye Education Analytics LLC ("we," "us," "our") develops Precision Start, a teacher-facing math intervention planning tool. We are based in Washington, DC.

**What Precision Start does:** We help K-8 math teachers identify which prerequisite skills their students are missing before a unit begins. The system groups students by shared needs and generates matched intervention plans. Teachers use this to plan targeted instruction from Day 1 of a unit instead of spending weeks figuring out who needs help.

**What Precision Start does NOT do:** We do not grade students. We do not make placement decisions. We do not replace teacher judgment. The system recommends; the teacher decides.

## 2. What Data We Collect

---

### 2.1 Student Data (Provided by Teachers and Schools)

- Student first and last names
- Assessment performance data (mastery levels, misconception categories)
- Prerequisite skill gap analysis results
- Tier classifications and instructional grouping assignments
- Checkpoint assessment scores and progress monitoring data

### 2.2 Teacher and Administrator Data

- Name, email address, school affiliation
- Override decisions and instructional notes
- Session feedback ratings and lesson completion tracking

## 2.3 What We Do NOT Collect

- Social Security numbers
- Home addresses or phone numbers
- Parent or guardian contact information
- Disciplinary records or health records
- Biometric data
- Browsing history or tracking cookies

## 2.4 Optional Demographic Data (School-Controlled)

We do not collect demographic data by default. Schools may opt in to share demographic data to enable equity analytics. When shared:

- Schools control which categories to share (accommodation status, demographic identifiers, socioeconomic indicators)
- Demographic data is never sent to third-party services paired with student names or identifiers
- Aggregate demographic statistics may be used for cross-school equity analysis with minimum group size ( $n \geq 5$ )
- Schools can revoke sharing at any time; data is purged within 30 days of revocation
- Enabling or disabling is done through school administrator settings
- No teacher-level access to raw demographic data

## 2.5 Automatically Collected Data

- Anonymous page-level analytics via Vercel Web Analytics (no cookies, no PII, GDPR-compliant)
- Error logs for debugging (may include technical identifiers, never student names)

# 3. How We Use Data

---

## 3.1 Primary Use

All data is used exclusively for educational purposes:

- Classifying students into instructional tiers
- Tracing skill gaps through prerequisite chains
- Grouping students by shared needs
- Generating intervention plans, assessments, and teacher supports
- Tracking progress through checkpoint assessments
- Equity analysis (opt-in only)

### **3.2 System Improvement**

We use data within each school's own tenant (automated, not manual) to track intervention effectiveness, calibrate confidence scoring, and improve classification accuracy. Cross-school analytics use only de-identified aggregates with minimum group sizes.

### **3.3 What We Never Do**

- Sell, rent, or trade student data
- Use data for advertising or marketing
- Build behavioral profiles unrelated to instruction
- Share identifiable data across schools
- Train any third-party AI model on student data

## **4. Data Processing and Student Privacy**

---

### **4.1 Not Sent to Third-Party Services**

Direct student-identifier fields — a student's name, ID number, email address, or a parent's contact information — are not interpolated into AI prompts by design (including for Anthropic or any future provider). Individual demographic data is never sent alongside identifying information.

An automated redaction layer additionally strips email, phone, and SSN patterns from any free text, and best-effort redacts the group's student names from free-text fields before they reach the AI.

### **4.2 Sent to Third-Party Services**

When generating intervention plans, the system sends:

- Tier classification (e.g., "Emerging")
- Instructional approach (e.g., "Representational")
- Math standard codes and descriptions
- Misconception types (e.g., "conceptual error")
- Number of students in a group
- Confidence scores
- Educator-authored instructional free text (e.g., academic-language notes, teacher lesson notes), passed through the automated redaction layer above

This is enough for the AI to generate useful content without knowing who any student is.

## 5. Data Sharing

---

We share data only with the service providers listed in our Subprocessor List. We do not sell data. We do not share data with other schools (individual data never shared; de-identified aggregates may be analyzed cross-school for participating schools). We disclose data if required by law.

## 6. Data Storage and Security

---

All data is stored in Google Cloud (Firebase) with AES-256 encryption at rest and TLS encryption in transit. Our Firestore security rules deny all direct client-side reads and writes. All access goes through server-side API routes. See our Security Overview for complete technical details.

## 7. FERPA Compliance

---

We operate as a "school official" with a "legitimate educational interest" under FERPA. We process only the minimum data necessary. Schools own their data. See our FERPA Compliance Statement for details.

## 8. COPPA Compliance

---

Students never access or use Precision Start. All data is provided by teachers and administrators. Because we do not collect information directly from children, COPPA's direct-collection requirements do not apply.

## 9. Data Retention

---

- **Active service:** Data retained for the duration of the school's service agreement
- **End of service:** All student data deleted within 60 days unless the school requests earlier deletion or export
- **Audit logs:** Retained for service period plus 1 year
- **Demographic data:** Purged within 30 days of revocation

## 10. Cross-School Data

---

Individual data is never shared across schools. De-identified aggregates may be analyzed across participating schools (opt-in) with minimum group size ( $n \geq 5$ ).

## 11. Your Rights

---

**Teachers:** Override any classification. View all data for their classes. Modify student records.

**Schools:** Own all data. Request export or deletion anytime. Request audit logs. Opt out of cross-school analytics.

**Parents:** Direct questions to the school, which manages records under FERPA.

## 12. Changes to This Policy

---

Material changes are communicated to schools at least 30 days before taking effect.

## 13. Contact

---

Andre Aina, Third Eye Education Analytics LLC [andre@thirdeyeanalytics.org](mailto:andre@thirdeyeanalytics.org)

# FERPA Compliance Statement

**Precision Start™ by Third Eye Education Analytics LLC Last Updated: August 31, 2026**

This statement summarizes how Precision Start™ complies with the Family Educational Rights and Privacy Act (FERPA, 20 U.S.C. § 1232g; 34 CFR Part 99). It is intended for school general counsel and compliance officers reviewing the platform.

## 1. School Official Designation

---

Third Eye Education Analytics LLC ("Provider") operates as a **school official with a legitimate educational interest** under FERPA's school official exception (34 CFR 99.31(a)(1)).

**Legitimate Educational Interest:** Provider's role is limited to delivering diagnostic skill grouping and intervention planning services that the school would otherwise perform internally. Provider analyzes pre-unit assessment data to identify prerequisite skill gaps, groups students by shared instructional need, generates intervention lesson plans, and tracks intervention effectiveness -- all functions that directly support the school's educational mission.

**Supporting Activities:** A Data Processing Agreement (DPA) is executed with each school before any student data enters the system. The DPA codifies:

- The educational purpose of the data processing
- Direct control by the school over its data
- Restrictions on re-disclosure
- Use limitations matching FERPA's school official requirements

## 2. FERPA Compliance Framework

---

### 2.1 Direct Control by the School

The school maintains direct control over Provider's processing of Student Data:

- Schools authorize which staff can access the platform

- Schools determine which students' data is processed
- Schools control demographic data sharing through opt-in settings
- Schools can opt out of cross-school analytics at any time
- Schools may request data export, modification, or deletion at any time
- Schools own all Student Data; Provider acquires no ownership rights

## 2.2 Use Limitation

Student Data is used **only** for the educational purposes described in the DPA: skill-based tier classification, prerequisite skill gap analysis, instructional grouping, intervention plan generation, progress monitoring and RTI documentation, within-school analytics for system improvement, and equity reporting (when opted in).

Student Data is **never** used for advertising, marketing, commercial profiling, sale to third parties, training of any third-party AI model, or any purpose unrelated to instructional planning.

## 2.3 No Re-Disclosure

Provider does not re-disclose Student Data to third parties except to subprocessors under contractual obligations consistent with FERPA, when required by law, or with the school's explicit written authorization.

## 2.4 Audit Trail

Every access to Student Data is logged with user identity, action taken, resource accessed, school context, and timestamp. Audit logs are available to schools upon request.

# 3. Specific FERPA Provisions

---

## 3.1 Education Records (34 CFR 99.3)

Provider processes records that meet the FERPA definition of "education records." Provider maintains these records on behalf of the school.

## 3.2 Personally Identifiable Information (34 CFR 99.3)

Provider processes: student names, assessment performance data, tier classifications, group assignments, and progress monitoring data.

Provider does NOT process: Social Security numbers, dates of birth, parent contact information, disciplinary records, health records, or any PII beyond what is necessary for instructional grouping.

### 3.3 Directory Information (34 CFR 99.37)

Provider does not designate any data as "directory information" or release any data in directory information format.

### 3.4 Parental Rights (34 CFR 99.10-99.22)

Provider supports schools in fulfilling parental rights under FERPA:

- **Right to inspect and review:** Schools can export complete student records
- **Right to request amendment:** Schools can modify records within the platform
- **Right to consent to disclosure:** Provider does not disclose data without school authorization
- **Right to file a complaint:** Provider supports schools in responding to complaints

### 3.5 De-Identification (34 CFR 99.31(b))

Cross-school analysis uses de-identified data with minimum group size ( $n \geq 5$ ). De-identification follows the FERPA standard.

## 4. Data Subject Categories

| Category           | Examples                                   | FERPA Treatment               |
|--------------------|--------------------------------------------|-------------------------------|
| Student PII        | Names, assessment results, classifications | Education records under FERPA |
| Teacher data       | Names, emails, override decisions          | Not student records           |
| Administrator data | Names, emails, processing actions          | Not student records           |

|                           |                                            |                                                        |
|---------------------------|--------------------------------------------|--------------------------------------------------------|
| Demographic data (opt-in) | IEP/504/EL status, race, ethnicity, gender | Education records when linked to identified students   |
| Audit log data            | User actions and timestamps                | Education records when referencing identified students |

## 5. State Law Compliance

Provider complies with the District of Columbia Student Data Protection Act and other applicable state student privacy laws.

## 6. Provider's FERPA Commitments

Third Eye Education Analytics LLC commits to: (1) operating as a school official under FERPA, (2) using data only for educational purposes, (3) maintaining school control, (4) limiting access to authorized personnel and automated systems, (5) providing audit logs on request, (6) supporting parental rights, (7) restricting re-disclosure, (8) notifying of compelled disclosures, (9) returning or deleting data on request, and (10) cooperating with DOE investigations.

## 7. Documentation and Verification

Schools may request: the DPA, Privacy Policy, Subprocessor List, Security Overview, Breach Notification Plan, audit log samples, and vendor security questionnaire responses.

## 8. Contact

Andre Aina, Principal -- Third Eye Education Analytics LLC -- [andre@thirdeyeanalytics.org](mailto:andre@thirdeyeanalytics.org)

# Security Overview

**For school IT and security review teams Third Eye Education Analytics LLC | Last Updated: August 31, 2026**

This document summarizes the technical and administrative security measures protecting Precision Start™.

## 1. Infrastructure

| Component           | Provider                                        | Region                  |
|---------------------|-------------------------------------------------|-------------------------|
| Authentication      | Firebase Authentication (Google Cloud)          | United States           |
| Database            | Firestore (Google Cloud)                        | United States           |
| File Storage        | Firebase Storage (Google Cloud)                 | United States           |
| Application Hosting | Vercel                                          | United States           |
| Assessment Scoring  | EdLight, PBC (subprocessor engaged by Provider) | Not specified by vendor |

Google Cloud and Vercel host in the United States and both maintain SOC 2 Type II certifications. EdLight, PBC, our assessment scoring subprocessor, has not specified a data processing location. Scanned student work sent to EdLight for scoring may contain handwritten student names; schools contract with Provider only, and Provider remains responsible to the school for that processing.

## 2. Data Security

### 2.1 Encryption

- **In transit:** All traffic encrypted via TLS 1.2+ (HTTPS)
- **At rest:** AES-256 encryption via Google Cloud's default encryption

### 2.2 Database Access Control

- All database reads and writes flow through server-side API routes using the Firebase Admin SDK
- Firestore security rules deny all direct client-side reads and writes
- Student work files are served through signed URLs with time-limited expiration
- The client-side Firebase SDK is used only for authentication and file uploads to Firebase Storage

## 2.3 Authentication

- Every API request requires a valid Firebase ID token verified server-side
- Edge middleware rejects requests without valid authorization headers
- Teachers join schools through single-use, transactional invite codes
- Failed authentication attempts are rate-limited

## 2.4 Authorization

- Teacher access is scoped to their own school and their own classes
- Coach access is scoped to assigned classes within a school
- School Administrator access is scoped to their assigned school(s) only
- Platform Administrator access (Provider personnel) is limited to one individual

## 2.5 Multi-School Isolation

Each school's data is strictly isolated. Every API route validates that the requesting user has been granted access to the specific school. **There is no path through which one school's staff can access another school's data.**

# 3. Application Security

---

## 3.1 Security Headers

All HTTP responses include: `X-Content-Type-Options: nosniff`, `X-Frame-Options: DENY`, `X-XSS-Protection: 1; mode=block`, `strict Referrer-Policy`, and restrictive `Permissions-Policy`.

## 3.2 Rate Limiting

| Endpoint Category | Limit              |
|-------------------|--------------------|
| AI generation     | 10 requests/minute |
| File uploads      | 5 requests/minute  |
| Authentication    | 10 requests/minute |
| General API       | 60 requests/minute |

### 3.3 Input Validation

All inputs are validated server-side. Database queries use parameterized operations. File uploads validate MIME types and file size limits.

## 4. AI Service Security

### 4.1 Not Sent to AI Services

Direct student-identifier fields — student names, student IDs, email addresses, parent contact information — are not interpolated into AI prompts by design, and individual demographic data is never sent alongside identifying information. An automated redaction layer strips email, phone, and SSN patterns from free text and best-effort redacts the group's student names from free-text fields. Name redaction is best-effort matching against the group roster, not a guarantee.

Every AI prompt file includes a documented "PII Guard" comment. All prompt files have been verified.

### 4.2 Sent to AI Services

Tier classifications, math standard codes, misconception types, student counts per group, aggregate confidence scores, and educator-authored instructional free text (passed through the redaction layer above).

### 4.3 AI Provider Training Policy

Anthropic contractually commits that data submitted via its API is not used to train its models (Anthropic Commercial Terms, Section 5).

## 4.4 Pseudonymization

A formal pseudonymization module can replace student names with generic identifiers (S001, S002, etc.). It is available for future features that would process student-level data.

## 5. Audit and Monitoring

---

Every significant action is logged: login events, report viewing, tier overrides, publishing, AI generation, group moves, checkpoints, uploads, school joins, gap events, and profile creation.

Each entry captures: who, what, which resource, which school, and when.

## 6. Personnel Controls

---

Production access is limited to the Provider's principal (Andre Aina). No contractors have direct access to Student Data. Backup Incident Commander: LeShae Daniel (Partner).

## 7. Compliance Status

---

| Framework                      | Status                                         |
|--------------------------------|------------------------------------------------|
| FERPA                          | Aligned                                        |
| COPPA                          | Not directly applicable                        |
| DC Student Data Protection Act | Compliant                                      |
| SOC 2 (Precision Start)        | Not held. No audit date to share at this time. |
| ISO 27001                      | Not pursuing at this time                      |
| FedRAMP                        | Not pursuing at this time                      |

## 8. Incident Response

---

Provider commits to: notifying affected schools within 72 hours (or sooner per law), providing written notification, cooperating with school notifications, and delivering a post-incident report within 30 days.

## 9. Insurance

---

Cyber liability coverage details and certificates of insurance are provided on a school-by-school basis during procurement. Request them at [andre@thirdeyeanalytics.org](mailto:andre@thirdeyeanalytics.org).

## 10. Vendor Review Cooperation

---

Provider welcomes: vendor security questionnaires (HECVAT, SIG), additional technical detail, penetration testing coordination, and review of specific concerns.

## Contact

---

Andre Aina, Principal -- Third Eye Education Analytics LLC -- [andre@thirdeyeanalytics.org](mailto:andre@thirdeyeanalytics.org)

# Subprocessor List

## Third Eye Education Analytics LLC Effective Date: July 15, 2026

This document lists all third-party services that process data on behalf of Third Eye Education Analytics LLC ("Provider") in connection with the Precision Start platform.

### Active Subprocessors

| Subprocessor            | Service                                               | Data Accessed                                                                                            | Location      |
|-------------------------|-------------------------------------------------------|----------------------------------------------------------------------------------------------------------|---------------|
| Google Cloud (Firebase) | Auth, database, file storage                          | Student Data (encrypted)                                                                                 | US            |
| Vercel Inc.             | App hosting, analytics                                | Anonymous traffic only                                                                                   | US            |
| Anthropic PBC           | AI content generation                                 | De-identified instructional metadata only (direct identifiers kept out of prompts + automated redaction) | US            |
| Resend Inc.             | Email notifications                                   | Teacher/Admin emails                                                                                     | US            |
| EdLight, PBC            | Assessment scoring (subprocessor engaged by Provider) | Scanned student work, which may include handwritten student names, and roster identity                   | Not specified |

### Data Transmission Summary

**Receive Student PII:** Google Cloud (Firebase), EdLight

**Receive de-identified data only:** Anthropic Claude

**Receive no student data:** Vercel, Resend

### AI Training Restrictions

Anthropic contractually commits that data submitted via its API is not used to train its models. Provider will notify schools immediately if any subprocessor changes its training

data policy.

## Subprocessor Changes

---

Provider commits to: 30 days advance notice for new subprocessors with Student Data access, allowing schools to object, and maintaining this list within 7 days of changes.

## Contact

---

Andre Aina -- Third Eye Education Analytics LLC -- [andre@thirdeyeanalytics.org](mailto:andre@thirdeyeanalytics.org)

# Breach Notification Plan -- Summary

## Severity Levels:

| Level           | Definition                                                 | Response Time   |
|-----------------|------------------------------------------------------------|-----------------|
| <b>Critical</b> | Confirmed unauthorized access to identifiable Student Data | Within 1 hour   |
| <b>High</b>     | System compromise with potential data path                 | Within 4 hours  |
| <b>Medium</b>   | Suspected breach or system anomaly                         | Within 24 hours |
| <b>Low</b>      | Incident with no evidence of data access                   | Within 72 hours |

## 5-Phase Response

1. **Contain** (0-4 hrs): Identify vector, revoke credentials, preserve evidence
2. **Assess** (4-24 hrs): Review logs, identify affected schools and data, determine scope
3. **Notify** (within 72 hrs of discovery, or sooner if required by law): Affected schools, regulators, school's parental contacts
4. **Remediate** (1-30 days): Implement fix, verify, prevent recurrence
5. **Post-Incident Report** (within 30 days of resolution): Written report with timeline, root cause, remediation, lessons learned

## Notification Recipients

- Affected School/District contacts (within 72 hours)
- DC OSSE (per DC Student Data Protection Act)
- Other state regulators as applicable
- Affected individuals (school-led, with Provider support)

## Incident Response Team

- **Incident Commander:** Andre Aina, Principal

- **Backup Incident Commander:** LeShae Daniel, Partner
- **External Legal Counsel:** Education data privacy attorney (engaged on retainer)

For the complete Breach Notification Plan, contact [andre@thirdeyeanalytics.org](mailto:andre@thirdeyeanalytics.org).

# Data Processing Agreement

Our Data Processing Agreement (DPA) is delivered directly to school and district contacts during the procurement process -- not included in this public trust packet. This ensures each agreement is reviewed by the correct contact at your organization and tailored to your jurisdiction's specific requirements.

## To Request the DPA

---

Contact:

**Andre Aina, Principal** Third Eye Education Analytics LLC [andre@thirdeyeanalytics.org](mailto:andre@thirdeyeanalytics.org)

When requesting, please include:

- Your school or district name
- Your role and decision-making authority
- Whether your organization uses the SDPC National DPA framework, a state-specific template (e.g., DC, NY Ed Law 2-d), or a custom DPA template

We will respond within 2 business days with the appropriate documentation, ready for your general counsel's review.

## What's in the DPA

---

Our DPA addresses:

- FERPA "school official" framework
- Specific permitted and prohibited uses of Student Data
- Subprocessor management and notification
- Data security commitments
- Breach notification timelines (aligned with applicable law)
- Data retention and deletion timelines
- Within-school analytics and opt-in cross-school analytics

- Demographic data handling (school-controlled opt-in)
- School/District rights, including data ownership, export, and deletion
- COPPA compliance
- State privacy law compliance
- Term, termination, and survival provisions

The DPA is modeled after the Student Data Privacy Consortium (SDPC) National Data Processing Agreement framework and can be substituted with the SDPC National DPA upon request.