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.

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.

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