

Student Data Transparency Notice

Multi-Headed Learning Engine (MHLE) — Georgia SDPAT Disclosure

Document Version	1.0
Effective Date	July 1, 2026
Governing Law	Georgia Student Data Privacy Act and Transparency (SDPAT), O.C.G.A. § 20-2-666 et seq.; FERPA
Document Owner	MHLE Data Privacy & Compliance
Contact	privacy@mhle.app

Contents

1. Overview

2. What Student Data We Collect

3. How We Use Student Data

4. Who Can See Student Data

5. Student and Parent Rights
6. Data Retention

7. Security Measures

8. Contact and Complaints

9. Updates to This Notice

Overview

This Student Data Transparency Notice ("Notice") describes how Multi-Headed Learning Engine (MHLE) collects, uses, shares, and protects student data when schools and districts contract with MHLE to provide educational technology services.

MHLE is an AI-powered cognitive learning platform that helps students take better notes, analyze their thinking, and build learning portfolios. When a school or district ("Institution") licenses MHLE, MHLE acts as a **school official** under FERPA and a **school service contractor** under Georgia SDPAT. That means we are legally required to protect student data, use it only for the purposes the school authorizes, and never sell or monetize it.

This notice is written in plain language so that parents, students, and administrators can understand exactly what data we handle and why.

Section 1 — What Student Data We Collect

MHLE collects four types of student data. We only collect what is necessary to run the platform and deliver the educational service.

1.1 Student-Provided Data

Information students enter themselves when using MHLE.

Data Element	What It Is	Why We Collect It
Name and email address	The student's display name and school email	Account creation and login
Research notes and written content	Text students type into the note editor	Core product feature — the notes are what MHLE analyzes
Uploaded documents and files	PDFs, images, or other files students attach to notes	Enables document-based analysis
Portfolio entries	Skills and achievements students choose to record	Building a learning portfolio
Student interests (middle school)	Topics a student selects during onboarding	Personalizing age-appropriate content

1.2 Auto-Generated Data

Data the platform creates automatically as a student uses it.

Data Element	What It Is	Why We Collect It
AI analysis results	The platform's multi-perspective analysis of a student's note	Core learning feature — helps students see multiple viewpoints
Rigor scores	An automatic score measuring depth of thinking in a note	Shown on the instructor dashboard to flag students who may need support
Gap analysis results	Identifies concepts a student has not yet addressed	Helps students self-direct their learning
Learning artifacts	Study plans, concept summaries, and synthesis documents generated from notes	Portfolio and study support
Health score	A composite measure of a student's recent engagement and note quality	Shown to instructors to trigger early-intervention alerts
Gamification data (middle school)	Points, tree stage, and activity milestones	Engagement and motivation for younger students
Brain state (middle school)	An emotional state check-in ("focused," "tired," etc.) entered before a Brain Break activity	Learning optimization; never used for disciplinary purposes
Exit-ticket responses (Weekly Learning Cycle)	A student's answers and score on a short end-of-lesson formative check, always tied to the student's account (never anonymous)	Shows instructors per-standard mastery so they can adjust instruction; visible only to the student's instructor and institution — never to other students. Collected only from students actively enrolled in an

Data Element	What It Is	Why We Collect It
		onboarded classroom; never collected on public share links

1.3 Instructor-Entered Data

Data created by teachers or administrators within MHLE.

Data Element	What It Is	Why We Collect It
Instructor observations	Notes, ratings, and tags a teacher attaches to a student's record	Student monitoring and progress tracking
Instructor alerts	System-generated notifications sent to a teacher about a student	Flags students whose engagement drops below a threshold
Enrollment records	Which classroom a student is enrolled in, and their enrollment date	Institutional record-keeping and course access control

1.4 Behavioral / Usage Data

Data about how a student interacts with the platform.

Data Element	What It Is	Why We Collect It
Feature interaction logs	Which buttons a student clicks, which analyses they run	Platform improvement and support troubleshooting
Session metadata	Login timestamps and session duration	Security monitoring and usage reporting to the Institution
Analysis request history	A log of which AI analyses a student has requested	Helps track progress over time

Section 2 — How We Use Student Data

Permitted Uses

- Providing the MHLE platform service to the student and their Institution
- Delivering AI-powered analysis, gap analysis, and learning artifacts to the student
- Displaying student engagement and progress data on instructor dashboards (within the same Institution)
- Sending transactional emails required by the service (e.g., account verification, parental consent requests for minors)
- Maintaining platform security, detecting abuse, and troubleshooting technical issues
- Responding to FERPA and SDPAT data subject rights requests
- Complying with legally required court orders or government mandates (with notification to the Institution wherever lawful)
- Providing aggregate, non-identifiable analytics to the Institution about overall platform usage

Prohibited Uses

- **Selling student data** — We do not sell, rent, lease, or trade student data to any third party
- **Behavioral advertising** — We do not use student data to build advertising profiles or serve targeted ads to students
- **Training AI models** — Student data is never used to train, fine-tune, or improve any AI model, including those of our AI providers (OpenAI, Anthropic, Google, Perplexity)
- **Profiling for non-educational purposes** — We do not create profiles of students for employment, credit, insurance, or any purpose unrelated to education
- **Sharing with unauthorized third parties** — We do not share identifiable student data without the Institution's written consent
- **Combining with external data** — We do not combine student records with data purchased from data brokers or marketing databases

Section 3 — Who Can See Student Data

3.1 The Student

Each student can see their own notes, analysis results, gap analysis, and learning artifacts within the MHLE platform. Students cannot see other students' data.

3.2 The Institution (Instructors and Administrators)

Instructors enrolled in a classroom can see the notes, rigor scores, health scores, and engagement data for students enrolled in that classroom. School administrators designated by the Institution can access Institution-wide reporting. Access is strictly scoped — instructors cannot see data from classrooms they do not teach.

3.3 Parents of Minor Students

Parents who have completed the parental consent workflow can view their child's engagement data and contact the school. MHLE supports FERPA parental access rights on request through the Institution.

3.4 MHLE Personnel

MHLE employees and contractors with a legitimate operational need (e.g., technical support, security incident response) may access student data. All such personnel are bound by confidentiality obligations. Access follows the principle of least privilege — we grant only the minimum access needed for the specific task.

3.5 AI Sub-processors (Transient Processing Only)

When a student's note is analyzed, the content is transmitted to one or more AI providers to generate the analysis. These providers process data transiently under MHLE's instructions and do not retain it for their own purposes or for model training.

Provider	Purpose	No Model Training
OpenAI, L.L.C.	Multi-perspective analysis, simulations	☐ Confirmed
Anthropic, PBC	Learning artifact generation	☐ Confirmed
Google LLC (Gemini)	Multimedia processing, transcription, epistemology tagging	☐ Confirmed
Perplexity AI, Inc.	Fact verification (Weekly Pulse feature)	☐ Confirmed

3.6 Other Service Providers

Provider	Purpose
Replit / Cloud Infrastructure	Application hosting and database hosting (US-East region)
Mailjet (Sinch)	Transactional email delivery
Stripe, Inc.	Payment processing (teacher/administrator accounts only; no student payment data collected)

No student data is transferred outside the United States except for the transient API calls described above, all of which use US-based API endpoints.

Section 4 — Student and Parent Rights

4.1 Right to Access

Students (and parents of minor students) have the right to request a copy of the student data MHLE holds about them. Requests should be directed to the Institution, which will coordinate with MHLE.

4.2 Right to Correct

If student data held by MHLE is inaccurate, students or parents may request a correction through the Institution.

4.3 Right to Delete

Upon request from the Institution, MHLE will delete all student data associated with a student's account. Students who leave an Institution may also request deletion directly by contacting privacy@mhle.app with verification of their institutional affiliation.

4.4 Right to Opt Out of Non-Essential Data Collection

Georgia SDPAT and FERPA allow Institutions to restrict data collection beyond what is needed for the core service. Institutions may contact MHLE to configure data minimization settings for their deployment.

4.5 Parental Consent for Minors (COPPA)

For students identified as under 13 years of age, MHLE requires verified parental consent before the student account is activated. The consent workflow is initiated at registration and records the parent's email address, consent date, and IP address. No data is collected from a minor until consent is confirmed.

4.6 How to Exercise Rights

To exercise any of these rights:

- **Through your school:** Contact your school's technology coordinator or principal. The Institution has primary responsibility under FERPA for managing these requests.
- **Directly to MHLE:** Email privacy@mhle.app with your name, your school's name, and a description of your request. We will respond within 30 calendar days.

Section 5 — Data Retention

Data Category	How Long We Keep It	What Triggers Deletion
Student account and enrollment data	Duration of the Institution's active contract, plus up to 30 days after contract end	Institution contract termination or deletion request
Notes, analysis results, and artifacts	Duration of active enrollment, plus 30 days after account deactivation	Student account deletion or Institution data deletion request
Instructor observations and alerts	Duration of the active classroom term, plus 30 days	Classroom deletion or Institution data deletion request
Exit-ticket responses (formative assessment records)	Duration of the Institution's active contract, plus up to 30 days after contract end	Institution data deletion request (included in the standard deletion flow and Certificate of Deletion counts) or contract termination
Usage logs (session metadata, click logs)	12 months from collection date	Automatic rolling deletion
Security and audit logs	24 months (required for security incident investigation)	Automatic rolling deletion
Parental consent records	Duration of student's account, plus 3 years (regulatory compliance record)	Upon legal retention period expiry

Upon contract termination, MHLE will:

1. Stop all processing of the Institution's student data within **5 business days**.
2. Delete all student data (including backups) within **30 calendar days**.
3. Provide a Certificate of Deletion upon written request.

Institutions may request a data export before termination in JSON or CSV format.

Export requests must be submitted at least 15 business days before the scheduled end date.

Section 6 — Security Measures

Domain	Safeguard
Encryption in transit	All data moving between students' browsers and MHLE servers is encrypted with TLS 1.2 or higher.
Encryption at rest	All student data stored in MHLE's database is encrypted at rest using AES-256.
Access controls	Role-based access control (RBAC) ensures that only authorized personnel can access student data. Access is reviewed quarterly.
Authentication	JWT-based session authentication; bcrypt password hashing; multi-factor authentication available for institutional administrators.
Audit logging	All access to student data is logged with a timestamp and actor identity. Logs are immutable.
Vulnerability management	Automated dependency scanning and static code analysis run on every production deployment. Critical vulnerabilities are patched within 24 hours.
Penetration testing	Annual third-party penetration testing; findings remediated within 30 days for critical/high severity.
Breach notification	In the event of a confirmed data breach affecting student data, MHLE will notify the Institution within 72 hours of confirmation.
Infrastructure isolation	Production, staging, and development environments are fully isolated. No student data is present in non-production environments.

Full details are available in the MHLE Security Questionnaire and Data Processing Agreement, available to Institutions upon request at compliance@mhle.app.

Section 7 — Contact and Complaints

Primary Contact

Privacy and Compliance	privacy@mhle.app — response within 30 calendar days for rights requests; within 72 hours for breach notifications
Security Inquiries	security@mhle.app
Legal and Contract Inquiries	legal@mhle.app

Complaints

If you believe MHLE has handled student data in a way that violates this Notice, Georgia SDPAT, or FERPA, you may:

1. **Contact MHLE directly** at privacy@mhle.app. We will investigate and respond within 30 days.
2. **Contact your Institution's FERPA officer.** The Institution, as the FERPA-covered entity, has primary responsibility for student data rights.
3. **File a complaint with the Georgia Department of Education** if you believe a violation of Georgia SDPAT has occurred: www.gadoe.org
4. **File a complaint with the U.S. Department of Education** for FERPA violations: studentprivacy.ed.gov/file-a-complaint

Section 8 — Updates to This Notice

MHLE will update this Notice when our data practices change in a material way. We will:

- Post the updated Notice at `/docs/legal/student-data-transparency` at least **30 days before** any material changes take effect.
- Notify Institutions by email to the registered administrator address.
- Maintain a version history table (below) so Institutions can track what changed.

Continued use of MHLE by an Institution after the effective date of a material change constitutes acceptance of the updated Notice, unless the Institution objects in writing before the effective date.

Version History

Version	Effective Date	Summary
1.0	July 1, 2026	Initial release. Covers data categories, permitted/prohibited uses, data subject rights, retention schedule, security measures, and contact information. Drafted to comply with Georgia SDPAT and FERPA.

For privacy inquiries, contact: privacy@mhle.app

For compliance and audit inquiries, contact: compliance@mhle.app

© 2026 MHLE (Multi-Headed Learning Engine). This document is a public-facing compliance notice and may be shared with students, parents, and school administrators.