Security & Privacy FAQ for School Districts

Enterprise Cloud Architecture & Data Protection Overview

1. District data storage

All district data is hosted within **Microsoft Azure's U.S.-based data centers**, specifically in the **[US Region] Azure region**.

Our architecture leverages:

- **Azure Kubernetes Service (AKS)** for containerized application hosting
- **Azure Database for PostgreSQL – Flexible Server (Private Access)** for relational data storage
- **Azure Virtual Network (VNet) isolation** to restrict all database access to internal services only

Physical & Infrastructure Security

Microsoft Azure data centers provide:

- 24/7 physical security and surveillance
- Biometric access controls
- Redundant power, cooling, and networking
- SOC 1, SOC 2 Type II, ISO 27001, ISO 27018 compliance

Your district data resides in hardened, enterprise-grade infrastructure used by Fortune 500 companies and U.S. government agencies.

2. How data is synced from to our Student Information System (SIS)

We use industry-leading secure data integrators:

- **Edlink**
- **Clever**
- **ClassLink**

Security Controls

- OAuth 2.0 authentication (no password storage)
- Token-based access control
- District-controlled data scope selection
- Encrypted API-based data transfer (TLS 1.2+)

Key Assurance

We never:

- Access your SIS database directly
- Store SIS administrative credentials

All SIS data access is:

- District-authorized
- Auditable
- Revocable at any time via the integrator dashboard

3. Data encryption

Yes. Data is encrypted at multiple independent layers.

Encryption In Transit

All data transmitted between:

- User browsers and our platform
- Our application servers and Database systems
- Our systems and SIS integrators

is protected using:

- **TLS 1.2 or higher**
- Strong cipher suites
- Certificate-based authentication

This prevents:

- Packet sniffing
- Man-in-the-middle attacks
- Session hijacking

Encryption At Rest (Azure-Managed)

Our databases use **Azure Storage Service Encryption with AES-256**.

This includes encryption of:

- All database files
- Indexes
- Write-Ahead Logs (WAL)
- Automated backups
- Snapshots
- Replicated storage

Encryption keys are managed by Microsoft using hardened Key Management Systems (FIPS 140-2 compliant).

4. Database Architecture & Access Controls

Our Database environment operates in **Private Access mode**, meaning:

- The database has **no public internet endpoint**
- It is accessible only within a private Azure Virtual Network
- Only authorized application services may connect

Network-Level Protections

- VNet isolation
- Network Security Groups (NSGs)
- Firewall rules
- Private DNS resolution

Authentication Controls

- Encrypted connection strings
- Role-based database access
- Principle of Least Privilege
- Multi-Factor Authentication (MFA) for engineering access

5. Passwords protection

Passwords are never stored in plaintext.

We use:

- Industry-standard salted hashing algorithms (e.g., bcrypt/Argon2 equivalent)
- One-way cryptographic hashing
- Secure credential storage

Even internal staff cannot retrieve or view original passwords.

6. Access to student PII data

We operate under strict Least Privilege principles.

Internal Controls

- Production access restricted to a limited number of senior engineers
- Mandatory MFA for all privileged accounts
- Segregation of development and production environments
- Logged and auditable access trails

Data Usage Policy

We do not:

- Sell student data
- Use student data for advertising
- Share data with third parties beyond required operational processors (e.g., Azure hosting)

All student data is used strictly to provide contracted educational services.

7. Backups procedures

Azure automatically:

- Performs encrypted backups
- Replicates backups across redundant infrastructure
- Protects backups with the same AES-256 encryption standards

Backups are:

- Stored securely
- Encrypted at rest

- Retained per operational policy
- Protected from public access

8. SFTP and/or data extracts?

For districts requiring automated secure file exchange:

- SSH key-based authentication only (no password login)
- Isolated directory per district
- Network-restricted SFTP endpoint
- Automatic file purge after transfer
- Audit logging of transfer events

Authorized school/districts can also initiate manual data extraction via their administrative accounts

9. Vulnerability & Patch Management

We maintain continuous security monitoring.

Automated Security Controls

- Daily dependency vulnerability scanning
- GitHub security advisory integration
- Static code analysis
- Container image scanning
- Automated CI/CD patch deployment

Infrastructure Patching

- Azure-managed OS patching
- Kubernetes cluster patching
- Rolling container updates
- Zero-downtime deployments where possible

10. Database Security Hardening

Our Database configuration includes:

- Private network-only access

- Encrypted storage
- Encrypted backups
- Encrypted WAL logs
- Role-based access controls
- Regular security updates managed by Azure

Database activity is protected from:

- Public network exposure
- Direct external queries
- Anonymous access

11. District discontinues a license with Let's Go Learn

We follow a strict **Data Retention & Secure Deletion Protocol**:

- Logical deletion of district PII data within 30-90 days or as directed in the DPA.
- Removal of PII data from active production databases
- Removal of PII data from backups per retention cycle
- Secure purge procedures
- Optional Certificate of Data Destruction

12. Incident Response & Breach Notification

We maintain a formal Incident Response Plan that includes:

- Immediate containment procedures
- Forensic investigation
- Root cause analysis
- Remediation steps
- Executive review

If an unauthorized disclosure of PII is confirmed:

- Designated district contacts are notified within 24–48 hours
- Scope of exposure is documented
- Mitigation actions are shared
- Ongoing updates provided

13. Security Standards and Frameworks Adherence

Let's Go Learn
EMBRACE PRECISION

Let's Go Learn aligns its security architecture, operational processes, and data governance practices with recognized industry standards and regulatory frameworks applicable to K-12 educational institutions.

FERPA (Family Educational Rights and Privacy Act)

- Student records are treated as protected educational records.
- Data is used strictly for legitimate educational interest.
- Districts retain ownership and control of student data.
- Access controls ensure only authorized users may view student PII.

COPPA (Children's Online Privacy Protection Act)

- We operate under school-authorized consent models.
- We do not collect unnecessary personal information.
- We do not use student data for advertising or profiling.

SOPIPA (Student Online Personal Information Protection Act - California)

- No selling of student data.
- No targeted advertising.
- No behavioral profiling outside educational purposes.
- Data deletion upon contract termination.

Information Security Framework Alignment

While we are not currently claiming formal certification unless specified, our security program aligns with the principles of:

SOC 2 Type II (Security, Availability, Confidentiality)

Our operational controls reflect SOC 2 trust service criteria, including:

- Logical access controls
- Change management procedures
- Vulnerability management
- Incident response planning
- Infrastructure monitoring
- Secure SDLC practices

Our hosting provider, Microsoft Azure, maintains SOC 2 Type II certification.

ISO/IEC 27001 & 27018 Alignment (via Azure Infrastructure)

Let's Go Learn
EMBRACE PRECISION

Microsoft Azure infrastructure is certified under:

- ISO/IEC 27001 (Information Security Management)
- ISO/IEC 27018 (Protection of PII in public cloud)
- ISO/IEC 27701 (Privacy Information Management)

By hosting within Azure's certified infrastructure, we inherit strong physical and environmental security controls.

NIST Cybersecurity Framework (CSF) Alignment

Our security program follows the NIST CSF functional model:

NIST Function	How We Implement It
Identify	Asset inventory, risk assessments
Protect	Encryption, MFA, RBAC, network isolation
Detect	Continuous vulnerability scanning
Respond	Formal incident response plan
Recover	Encrypted backups & restore testing

Cryptographic Standards

Our encryption practices align with industry-recognized standards:

- AES-256 encryption for data at rest (Azure Storage Service Encryption)
- TLS 1.2+ for data in transit
- FIPS 140-2 validated cryptographic modules (via Azure infrastructure)
- Salted, adaptive hashing for password storage

Cloud Infrastructure Compliance (Microsoft Azure)

Microsoft Azure maintains compliance certifications including:

- SOC 1, SOC 2, SOC 3
- ISO 27001 / 27018 / 27701
- FedRAMP Moderate
- HIPAA/HITRUST (infrastructure eligible)
- CSA STAR

We leverage these enterprise-grade controls as the foundation of our hosting environment.

Let's GoLearn
EMBRACE PRECISION

Secure Development Practices

Our engineering processes follow secure software development lifecycle (SSDLC) best practices:

- Code review requirements
- Automated static code analysis
- Dependency vulnerability scanning
- Container image scanning
- CI/CD security gates
- Segregation of development and production environments

Data Governance Principles

We adhere to the following operational standards:

- Principle of Least Privilege
- Role-Based Access Control (RBAC)
- Multi-Factor Authentication for privileged accounts
- Network segmentation
- Audit logging and monitoring
- Data minimization
- Secure data destruction upon termination

Let's Go Learn
EMBRACE PRECISION

Quick Reference for IT Departments

Category	Standard
Hosting Provider	Microsoft Azure (U.S. Region)
Application Hosting	Azure Kubernetes Service (AKS)
Database	Azure PostgreSQL Flexible Server (Private Access)
Encryption (Transit)	TLS 1.2+
Encryption (Rest)	AES-256 (Azure Storage Encryption)
Backup Encryption	AES-256
Database Exposure	Private VNet Only (No Public Endpoint)
Authentication	OAuth 2.0 / SSO / MFA
SIS Integration	Clever, ClassLink, Edlink
Password Storage	Salted Hashing (One-Way)
Compliance Architecture	FERPA, COPPA, SOPIPA-aligned
Access Model	Least Privilege