Your students' data is protected.

Before you deploy AI at scale, your institution needs to know: where does the data go, who can access it, and what happens to it after? This document answers those questions. InStage is built for institutional procurement — with the governance, encryption, and data residency controls your compliance team expects.

No model training on student data
Student recordings, transcripts, and instructor materials are never used to train AI models — ours or our vendors'.

Encrypted in transit and at rest
All data is encrypted using TLS in transit and AES-256 at rest, with cryptographic keys managed in-region.

Jurisdiction-based data storage
Customer data is stored in-region on institutional-grade cloud infrastructure with encryption keys managed locally.

INCIDENT RESPONSE & INDEPENDENT TESTING

Incident Response Program
InStage maintains a documented incident response program with procedures for containment, investigation, and notification. Where a breach poses a real risk of significant harm, InStage follows applicable notification requirements and supports institutional obligations.

Third-Party Penetration Test
An independent web application penetration test was completed in August 2025, with a retest confirming full closure of findings in October 2025. InStage maintains a vendor and subprocessor program with documented data elements and regions.

ENCRYPTION & KEY MANAGEMENT

- **In transit:** TLS protects all data between users and the platform
- **At rest:** AES-256 encryption for databases, backups, and file storage
- **Key management:** Cryptographic keys stored in-region with role-based controls, rotation, and monitoring
- **Backups:** Encrypted and rotated on schedule; deletions propagate on backup expiry

SECURITY CONTROLS

- **Access:** Role-based (RBAC), least-privilege, MFA where supported
- **Endpoints:** Full-disk encryption required for staff with data access
- **Monitoring:** Centralized logging, security telemetry, threat detection
- **Development:** Code review, change control, vulnerability management, patching

DEFAULT RETENTION (INSTITUTION-CONFIGURABLE)

VIDEO RECORDINGS	AUDIO SESSIONS	TRANSCRIPTS
90 days	**12 months**	**12 months**
If enabled by institution	Default for voice-only	Searchable by staff

Administrators can shorten or extend retention and manage capture settings at the tenant level. Upon verified request, InStage will delete customer content subject to backup mechanics and lawful exceptions.

WHAT WE DO NOT DO

- **No AI training** on customer content — recordings, transcripts, or materials
- **No facial recognition,** biometric identification, or similar tracking
- **Not designed for PHI/ePHI** unless a separate written agreement is in place

Compliance & Testing: ✓ PIPEDA (Canada) · ✓ FERPA support (US) · ✓ SOC 2–aligned · ✓ Pen tested (2025) · ✓ Incident response program

Need the full due-diligence package?

Subprocessor list, data-location summary, pen test executive summary, retention schedule, and WebRTC voice processing attestation — available upon request by an authorized administrator.

privacy@instage.io
instage.io/security