Security and Compliance Summary

Atlas K-12 is on-premise only. Your data lives on your server. The table below lists the security features that are actually built and working in the product today. Atlas K-12 is founder-built software in active development: when more features land, they get added here, not before.

Category	What is built today
Authentication	Local username and password accounts with 8-hour session timeouts and brute-force lockout (five failed attempts per IP per 15-minute window). Single sign-on is scaffolded but not production-ready today.
Authorization	Role-based access control with four roles (teacher, counselor, admin, district admin) plus a Care Team coordinator flag. Per-school scoping and per-record visibility checks on every route that takes a student identifier.
Data at Rest	The database lives on your server. Full-disk encryption (BitLocker or equivalent) is the district IT team's choice at the host level. Backups are handled by your existing backup tooling, so they inherit whatever encryption your backup system already provides.
Data in Transit	TLS from the browser to Atlas, terminated by IIS on your server. The Compass AI process has no outbound network calls under normal operation, enforced by a process-level socket guard inside the Python runtime at application startup.
Audit Log	Every create, update, delete, and import operation is written to a local audit log with user, timestamp, and affected record. The log lives in your own database. There is no read-side access logging today.
Compliance	FERPA: district is the data controller, AtlasOA LLC is a school-official service provider. COPPA: no advertising, no resale of student data, ever. Aligned with California SOPIPA, Colorado HB14-1294, Connecticut SB949, and New York Education Law 2-d through the on-premise architecture.
Incident Response and Breach Notification	Atlas K-12 is deployed on hardware your district operates. Detection and response on the district network is part of your IT team's existing incident response process. AtlasOA LLC commits to notifying the Educational Agency within 72 hours of discovering any unauthorized access involving the Atlas K-12 codebase, AtlasOA LLC vendor systems, or AtlasOA LLC personnel. Notification includes the nature and scope of the incident, the categories of student data affected, and the mitigation steps in progress. See the Atlas K-12 Data Processing Addendum (Section 4A and Section 5) for the full division of security responsibilities between AtlasOA LLC and the Educational Agency.
Operational	On-premise only. No cloud subprocessors. No telemetry. No outbound calls under normal operation. Air-gap install option supported. Signed Windows installer built with Inno Setup and code-signed through Azure Trusted Signing.

WHAT YOUR IT TEAM OWNS

- Host hardening: OS patching, BitLocker, antivirus, Windows Firewall, the usual server baseline.
- Incident detection and response on district infrastructure. Atlas K-12 runs on your server, so your SOC or IT team is the first responder.
- Backups and restore testing. Atlas writes to a single data directory that drops into any backup system you already run.
- User provisioning and offboarding inside the Atlas admin screen.

WHAT WE OWN

- Patching the Atlas K-12 software itself through signed installer updates.
- Disclosing any security defect found in the Atlas K-12 code within 72 hours under the DPA.
- Keeping student data off of any cloud we operate. There is no cloud to keep it off of: the product has no server-side component.

AtlasOA LLC | 8112 Maryland Ave, Suite 400, St. Louis, MO 63105 | ashleyreddick@atlasoa.com | atlasoa.com

Questions: ashleyreddick@atlasoa.com | AtlasOA LLC, Missouri