AI that helps teachers, not a FERPA incident.

~62.4M claimed

Source: BleepingComputer, 2025. In the December 2024 PowerSchool breach, the threat actor claimed to have stolen records on 62,488,628 students and 9,506,624 teachers across thousands of districts. PowerSchool did not confirm a total affected, and per PowerSchool fewer than a quarter of involved individuals had Social Security numbers exfiltrated. One vendor incident reaches that far because student records concentrate in shared systems.

THE EXPOSURE

- **Student records in prompts.** Grades, IEPs, disciplinary notes, and identifying detail pasted into AI tools no one vetted, where it becomes an education-record disclosure under FERPA.
- **Shadow AI no one approved.** Unsanctioned assistants and command-line clients running across staff laptops, personal accounts, and browser sessions that never touch a sanctioned path.
- **Nothing to produce on request.** When a parent exercises a FERPA right, a state regulator opens a student-data-privacy inquiry, or the board asks what happened, there is no signed answer for what the AI was given or returned.

WHAT CHANGES WITH VERILLIAN

- **Student data is held at the boundary.** A sentinel on each device governs any tool that reaches a provider over HTTPS, with no per-tool integration, so requests are held to policy before they leave district or university systems.
- **Protected detail is redacted first.** Names, student IDs, and other identifiers are redacted or blocked before a request reaches a provider. Detection is best-effort and fails closed when uncertain, not a guarantee that every value is caught.
- **You hold the keys.** The record is encrypted under your own key, which is shipped today, on a server that stores ciphertext it cannot read. Even Verillian cannot read the content.
- **Tamper-evident proof.** Every captured interaction is signed on the device and hash-chained into an append-only record, verifiable mathematically and independent of vendor attestation, ready for a parent inquiry or an audit.

Built for FERPA and COPPA, and designed to align with state student-data-privacy laws. **The institution keeps custody of both the data and the record:** policy is enforced the moment a tool acts, and if no valid policy is present or the audit pipeline fails, AI traffic stops rather than sending student data ungoverned. The data you do not send cannot be breached, and the chain proves what was sent and what was redacted. The software is **source-available (Elastic License 2.0)**, so your IT and security staff can read exactly what runs on district and faculty machines.

Verillian, LLC. To scope a pilot in your own environment, under your own keys, name an institutional sponsor and a technical contact.

hello@verillian.ai