

How does Cyber Crucible support FERPA and student-data privacy for schools and universities?

Short answer: Cyber Crucible helps educational institutions two ways: it stops ransomware autonomously without a 24/7 security operations center, and — through FortressAI — it evaluates AI-tool data access on the device so student records and family data do not reach a public AI system by accident. Because analysis is local and no student records are collected, protected educational records stay within the institution's boundary.

The two education problems it addresses

- **Ransomware without a SOC.** Kernel-level prevention stops attacks in under 200 milliseconds with no analysts to hire and no round-the-clock monitoring contract to fund.
- **AI governance for the classroom.** FortressAI checks each prompt on the device, so protected educational records and personal family data are not sent to a public AI system — including as training data.

Vendor-selection notes

- Cyber Crucible acts as a school official / service provider under the institution's direction and does not use student data for any secondary purpose.
- State student-privacy laws (for example, in California, New York, and Colorado) layer additional vendor obligations; the local-processing, no-collection design supports them. Documentation is available under NDA.

Revision #2

Created 2026-07-23 15:18:22 UTC by Dennis Underwood

Updated 2026-07-23 18:19:52 UTC by Dennis Underwood