Guardian Compliance for K-12 Districts and Schools

How PTS Guardian tiers deliver the student data privacy, E-rate-ready cyber posture, and board-ready evidence your district needs to stay teaching.

The business problem: K-12 is now the #1 ransomware target sector in the United States. LAUSD, Minneapolis Public Schools, Clark County, and Baltimore County each lost millions in recovery or had hundreds of thousands of student records exposed. Districts carry the strictest student privacy obligations of any sector (FERPA, PPRA, CIPA, COPPA, plus a state-by-state patchwork) and the leanest IT teams to enforce them. Add 1:1 device programs, vendor sprawl across edtech, frequent staff turnover, and a school board that now asks the superintendent about cybersecurity every meeting.

The PTS answer: Guardian Compliance is our tier built for school districts that have to keep teaching, keep funding flowing, and keep student data protected, all at once. It combines our managed help desk, cybersecurity, backup, M365 E5 (or A5) cloud, and vCIO management with the Written Information Security Program, E-rate-ready documentation, and board-ready cyber posture reporting your superintendent and school board need. **Compliance is the tier that turns student privacy intent into documented evidence.**

THE SOLUTION

Why the Compliance tier

Compliance is the Guardian tier built end-to-end for school districts where student privacy, funding compliance, and teaching continuity all depend on the same security posture. Six capabilities make the difference:

- **M365 E5 or A5 with Purview, DLP, and Message Encryption.** Student-record data loss prevention, audit log retention, and encrypted external email. The control set FCC E-rate Cyber Pilot and CISA K-12 guidance now reference directly.
- **Written Information Security Program (WISP) and IR Plan.** Documented FERPA, CIPA, and state student data privacy policies. Maps to board governance reporting and state breach notification obligations. Includes superintendent escalation tree.
- **Air-gapped monthly server backups, performed and tested by PTS.** Demonstrable ransomware recovery posture. The single most effective control against the wave that hit LAUSD, Minneapolis, Clark County, and Baltimore County. Restore testing logged.
- **Phishing-resistant MFA on every staff and admin account.** Email, VPN, SIS, gradebook, finance, and admin SaaS via SSO. The most-exploited gap in K-12 ransomware. Required language in the E-rate Cyber Pilot eligible services list.
- **Edtech sub-processor and vendor inventory with annual reviews.** LMS, SIS, gradebook, classroom apps, assessment, parent comms, 1:1 device management: all touch student PII. PTS maintains the inventory, COPPA-compliant contract review, and annual log.
- **Annual training, phishing simulation, and tabletop exercise.** Staff, administrators, and IT awareness. Documented completion records retained for school board review, state audit, and E-rate program file.

WHAT YOU GET

Inside the Compliance tier

A single managed-service bundle that delivers the help desk, security, backup, M365 cloud, and vCIO management your district's FERPA, CIPA, and E-rate obligations depend on. Each layer is included in the monthly fee.

Service Layer	What you get
Help Desk	Remote, on-site, and emergency support within monthly limits. Acknowledge under 1 business hour, on-site under 8 business hours. 25% discount on after-hours emergency. Coverage scales to back-to-school, testing windows, and exam periods.
Cybersecurity	Advanced endpoint detection and response, 24/7 managed detection and response, phishing simulations and training, application allow-listing, DNS and CIPA-aligned content filtering, full-disk endpoint encryption, SIEM with compliance logging.
Backup	Image-based cloud backup (workstations and servers), 3x 2TB external drives included, monthly air-gapped server backups performed by PTS, monthly restore testing logged for school board, state audit, and E-rate program file.
Cloud (M365 E5 or A5)	M365 E5 or A5 academic licensing where eligible, Purview audit logs, DLP for student PII patterns, Message Encryption, email and file backup, DDoS protection, DNS and domain management.
vCIO / IT Leadership	Quarterly TBR, PTS firewall and network standards, edtech vendor and sub-processor management, 100+ policy templates including WISP, FERPA, CIPA, AUP, BYOD, and IR Plan. Annual written cyber posture report for the superintendent and school board.

Why one bundle, not piecemeal tools

Most districts run a patchwork: a CIPA filter from one vendor, endpoint software from another, a SIS provider, an LMS provider, a tech director balancing classroom support and backup tapes, and an AUP last updated five years ago. Guardian Compliance replaces that stack with one accountable provider whose evidence binder maps directly to FERPA, CIPA, E-rate program reviews, state student data privacy law, and your school board's cyber posture agenda item.

What it takes	Piecemeal	Phantom Bundle
Vendor count	6 to 10 separate contracts: MSP, SOC, EDR, backup, M365, training	One contract, one invoice, one accountable provider
Documentation	Tech director assembles WISP and AUP from each tool's docs	PTS maintains WISP, FERPA/CIPA policies, IR Plan, AUP
Restore testing	Backup vendor sells software; IT self-tests or skips	Monthly air-gapped restore performed and logged by PTS
E-rate / Cyber Pilot readiness	Tech director self-prepares Form 470, 471, 484 bids and scope	PTS supplies eligible-services scope, evidence, and program file
Edtech sub-processor accountability	Each LMS, SIS, classroom app tracked independently or not at all	PTS maintains COPPA-aware sub-processor inventory and reviews
Single point of escalation	Incident response routes through each vendor's separate support	P1-P4 escalation through one MSP, superintendent timeline day one

One contract. One WISP. One accountable provider. That is the difference between a tech stack and the documented student data stewardship FERPA, CIPA, and your school board now expect.

THE PROOF

The cost of getting it wrong

K-12 is the #1 ransomware target sector. Recovery costs reach $9.7M for a single mid-size district, and the average GAO range is $50K to $1M per incident. Beyond dollars: canceled classes, leaked Social Security numbers, state AG investigations, and a school board cyber audit that lands on the superintendent.

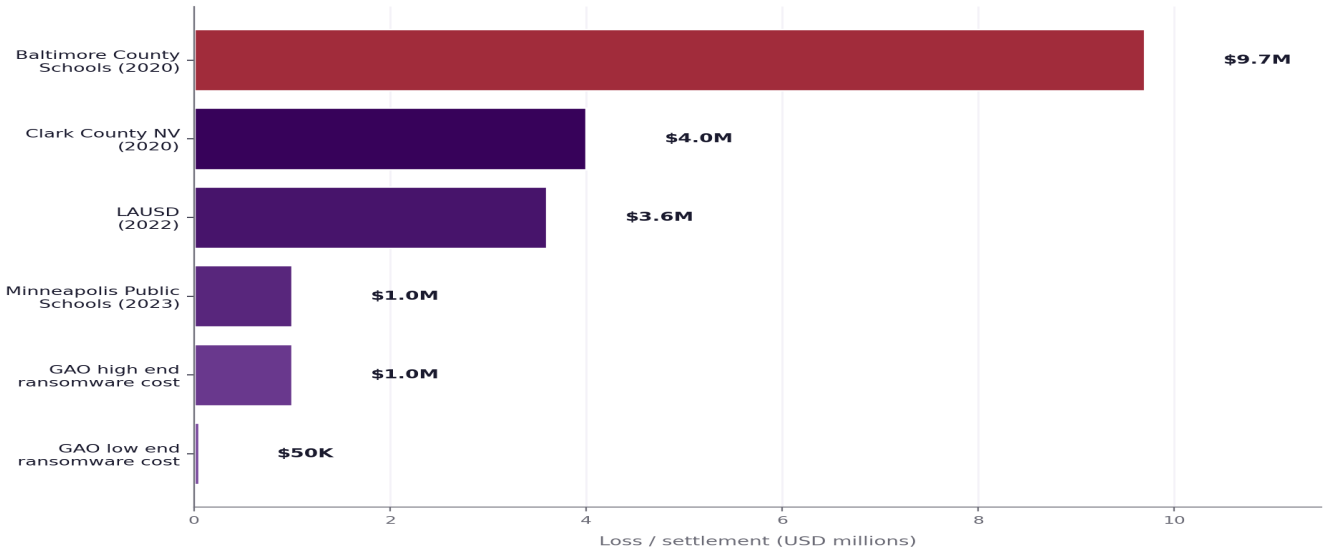
$9.7M
Baltimore County Public Schools 2020 recovery + upgrades cost

320K
Students locked out of school work in Clark County Nevada (2020)

$200M
FCC E-rate Cybersecurity Pilot funding now available to schools

#1
K-12 is now the most-targeted ransomware sector in the US

Public-record K-12 cyber impact.



Recovery costs and ransom demands from district press releases, state inspector general reports, GAO findings, and the FTC Illuminate Education complaint. Beyond the dollar figure, each district above also faced canceled classes, board cyber audits, state AG inquiries, and parent and staff PII exposure not captured in the disclosed number.

Three patterns we keep finding in K-12

PATTERN 01

MFA on email, not on the SIS or finance system

Staff email has MFA but the student information system, gradebook, and ERP/finance system are still password-only. The most-exploited gap in K-12 ransomware. Phishing-resistant MFA on every entry point, behind SSO, closes it.

PATTERN 02

Edtech vendor sprawl, no COPPA-aware inventory

LMS, SIS, gradebook, classroom apps, parent comms, 1:1 device MDM, and assessment platforms all touch student PII. Most districts have no current vendor inventory, no contract review, and no FERPA-compliant data sharing agreements on file.

PATTERN 03

Backups exist, but restore testing never happens

Cloud backup tool installed years ago, never actually restored from. The Illuminate Education and Baltimore County cases both exposed gaps between backup posture and restore posture. PTS tests restore monthly and logs the result.

THE DETAIL

Mapped to K-12 obligations and CIS Controls

Page 4 pairs each federal and state K-12 obligation with the Guardian capability that delivers it. Page 5 shows the CIS Controls v8.1 baseline (per the K-12 Companion Guide) that implements those obligations. Skim the Compliance column, every YES is documented and audit-ready.

FERPA AND PPRA - Federal student record privacy

Citation	Requirement	How Guardian Delivers	Co-Mgd	Fund.	Compl.
FERPA 99.31	Limit access to education records and PII from education records to authorized school officials with legitimate educational interest.	Role-based access via Entra ID, M365 conditional access, M365 Purview audit logs and DLP rules tuned to student PII patterns.	NO	PART	YES
FERPA 99.35	Reasonable methods to protect education records, including written agreements with vendors and re-disclosure controls.	Edtech sub-processor inventory, contracted data-sharing language, annual review log, vendor MFA and SSO enforcement where supported.	NO	PART	YES
PPRA	Notice and consent for surveys, evaluations, and the marketing use of student data.	Documented survey and assessment workflow in WISP, parental notification scaffold, and AUP language reviewed annually.	NO	YES	YES

CIPA, COPPA, AND STATE LAW - Filtering, under-13 consent, breach notice

CIPA	Internet safety policy with technology protection measures (filtering) for obscene and harmful content on minor-facing devices and networks.	DNS and content filtering with CIPA-aligned categories, documented internet safety policy, annual public review, AUP enforcement.	PART	YES	YES
COPPA	Verifiable parental consent or school-as-agent designation for any edtech vendor collecting PII from students under 13.	COPPA-aware edtech intake checklist, school-official designation language in vendor contracts, vendor list reviewed annually.	NO	PART	YES
State laws	State student data privacy laws (e.g. Indiana HEA 1486, CA SOPIPA, NY Ed Law 2-d) plus 50-state breach notification.	WISP aligned to state student data privacy law, documented IR Plan with state AG and parent notification scaffolds, training records.	NO	NO	YES

FCC E-RATE AND CYBER PILOT - Funding-ready posture

E-rate	Funding eligibility requires CIPA-compliant filtering, internet safety policy, public hearing or meeting, and program file documentation.	Documented filter posture, CIPA policy template, evidence binder, Form 470 and 471 scope and bid support, retention per USAC rules.	PART	YES	YES
Cyber Pilot	FCC Cybersecurity Pilot supports up to $40.80 per student over 3 years (pre-discount) for advanced firewall, endpoint, identity, MDR.	Eligible-services scope mapped to Compliance tier, Form 484 narrative support, eligible product evidence, FY-aligned procurement records.	PART	PART	YES

CIS 01-03 - Inventory of assets, software, and student data

CIS Control	Requirement	How Guardian Delivers	Co-Mgd	Fund.	Compl.
CIS 01	Inventory and control of enterprise assets connected to the district's infrastructure.	Full asset inventory in a secure documentation portal, M365 device inventory, 1:1 device MDM enrollment records, change-controlled.	YES	YES	YES
CIS 02	Inventory and control of software assets; only authorized software installed and executable.	Software inventory via RMM and centrally managed endpoint policy, application allow-listing on supported endpoints and 1:1 devices.	PART	YES	YES
CIS 03	Data protection: identify, classify, securely handle, retain, and dispose of student PII and education records.	BitLocker encryption, M365 Purview DLP, encrypted email, documented student PII data classification, secure media disposal.	PART	YES	YES

CIS 04-05 - Secure configuration and account management

CIS 04	Secure configuration of enterprise assets and software; patch and update systems.	Documented hardening baselines via Intune and group policy, patch management on supported endpoints, monthly compliance reporting.	YES	YES	YES
CIS 05	Account management: assign and manage credentials for staff, student, contractor, and service accounts.	M365 identity governance, designated admin accounts, enterprise password vault with rotation, joiner-mover-leaver workflow for staff and student matriculation.	YES	YES	YES

CIS 06-08 - Access control, awareness, audit logging

CIS 06	Access control: phishing-resistant MFA on all remote and admin access, role-based access, quarterly reviews.	Entra ID conditional access, phishing-resistant MFA on email, VPN, SIS, gradebook, ERP, and admin via SSO, quarterly access reviews.	YES	YES	YES
CIS 08	Audit log management: collect, alert, review, and retain audit logs.	SIEM with integrated compliance logging, M365 Purview audit log retention, 24/7 MDR, documented monthly log review.	PART	YES	YES
CIS 14	Security awareness and skills training: phishing-resistant culture, incident reporting, AUP enforcement.	Monthly phishing simulations for staff and admins, annual training, AUP review for staff and students, documented completion records.	YES	YES	YES

CIS 11 / 17 - Recovery and incident response

CIS 11	Data recovery: tested practices sufficient to restore in-scope assets to a pre-incident and trusted state.	Image-based cloud backup, monthly air-gapped server backups performed by PTS, monthly restore testing with documented log.	YES	YES	YES
CIS 17	Incident response: documented program to prepare, detect, and respond to attacks, including superintendent and board notification.	Documented IR Plan, P1-P4 playbooks, partner SOC threat response, superintendent timeline, annual tabletop exercise, state AG and parent notification scaffold.	PART	YES	YES

THE PATH FORWARD

What working with PTS looks like

Four stages, no surprises. Deployed Compliance posture in 30-90 days, E-rate and Cyber Pilot documentation in hand.

1
Discovery
60-min K-12 cyber and CIPA / E-rate readiness review.

2
Assessment
WISP and CIS gap snapshot, prioritized findings.

3
Implementation
Compliance tier deployed in 30-90 days. M365 E5/A5, SIEM, air-gapped backups, WISP, IR Plan.

4
Ongoing
Quarterly TBR, monthly air-gap testing, annual board cyber report.

Add a vCISO for board-level depth

For districts preparing for an E-rate Cyber Pilot award, a state audit, a 1:1 device program expansion, a SIS migration, or a school board cyber inquiry, a fractional **Phantom vCISO** engagement layers on board reporting, compliance roadmap, risk register ownership, and incident liaison. Tiers: Foundation, Operational, Strategic.

Common gaps we find in K-12

- MFA on staff email but not on SIS, gradebook, or ERP
- No COPPA-aware edtech vendor inventory or contract review
- CIPA filter in place but AUP and internet-safety policy stale
- Backups exist, but restore testing never performed
- Off-boarded staff and graduated students retain access
- No IR Plan with superintendent and board notification path

Important. K-12 compliance with FERPA, PPRA, CIPA, COPPA, state student data privacy laws, FCC E-rate program rules, and the FCC Cybersecurity Pilot is the responsibility of the district and its school board. PTS provides the technology, documentation, and program rigor that support those obligations. Board decisions and regulatory filings (including E-rate Forms 470, 471, 484, 486) remain with the district. PTS is not a law firm and does not provide legal or USAC consulting advice.

Next step: 30-minute K-12 Readiness Review

We walk your district environment against this exact mapping and leave you with a one-page gap snapshot and E-rate Cyber Pilot fit summary. No obligation.

Talk to PTS

hello@phantomts.com
phantomts.com/guardian

Why districts choose Phantom

Since 2010
OPERATING
Indiana-based MSP serving K-12 districts, nonprofits, and regulated SMB clients.

100+
POLICY TEMPLATES
WISP, FERPA, CIPA, and CIS v8.1-aligned policy library applied to every engagement.

24/7
MDR COVERAGE
Partner SOC monitoring, incident response runbooks, board-ready escalation.