TorchLight
Secured & Managed IT

BUILT FOR CALIFORNIA EDUCATION

Cybersecurity

Readiness Checklist

A leadership playbook aligned to FERPA, CIPA, and California Education Code requirements, plus the forward-looking controls auditors and insurers will be asking about next.

EDITION **6.2026** AUDIENCE **Cabinet, IT & Board / Trustees**
SCOPE **California K-12 Districts, Community Colleges & Independent Institutions**

RISK ALIGNED. REWARD DEFINED. SECURED & MANAGED IT

HOW TO USE THIS DOCUMENT

An audit-ready picture, in fifteen minutes.

This checklist is built for California education leaders, superintendents, presidents, business officers, IT directors, and the boards and trustees they answer to, who want a single sit-down view of where the institution stands against current privacy and security requirements and the threats that will define the next review cycle. Every item is auditable, and every item is something a trustee can ask about and an IT leader can answer with evidence.

Part I covers what the rules actually require: FERPA student-records obligations, the CIPA internet-safety conditions tied to E-Rate, the GLBA Safeguards Rule that now governs Title IV institutions, and California's own pupil-records and EdTech statutes (Education Code 49073.1 and SOPIPA). Part II covers what regulators and insurers do not all require yet but are increasingly asking about: phishing-resistant identity, ransomware resilience, AI-enabled fraud, and board cyber literacy.

Check the boxes you have evidence for. Anything unchecked is either a gap, an in-flight project, or a deliberate risk acceptance, and each deserves a documented owner and a date.

Same-Day
FSA BREACH REPORT TO ED

30-Day
FTC SAFEGUARDS NOTICE

79
AUDITABLE CONTROLS BELOW

PART I · REGULATORY REQUIREMENTS

What the rules actually require.

Eight cards mapping directly to FERPA, CIPA, the GLBA Safeguards Rule, and California's pupil-records and student-privacy statutes.

Every item here is auditable. Every item maps to a specific statute, regulation, or funding condition, and the AUTHORITY line at the bottom of each card tells you where. If a box is unchecked, treat it as a finding waiting to happen. If you have checked a box but cannot produce evidence, treat it the same way.

AT A GLANCE

Eight domains. 44 auditable controls, every one mapped to an authority.

APPLICABILITY MAP

Which requirements apply to you

Federal and California obligations by institution type.

	Public K-12	Private K-12	Community College	College / University
FERPA Student records	✓	◉	✓	✓
CIPA / E-Rate Internet safety	✓	◉	—	—
GLBA Safeguards Title IV aid data	—	—	✓	✓
CA Ed Code / SOPIPA Pupil data	✓	◉	◉	—
CA Breach Notice Civ. Code 1798.29 / .82	✓	✓	✓	✓

✓ Applies ◉ Conditional — Limited / rarely

Conditional = applies if you accept the related federal funds (E-Rate, Title IV) or serve K-12 students. Verify against your funding and programs.

Student Records & FERPA Governance

The annual obligations every California school and college already owes its students.

- ☐ Issue an annual FERPA notification of rights to inspect, amend, consent, and file a complaint, through a reasonable method such as a handbook, website, or mailing.
- ☐ Publish a directory-information notice listing each data element and give parents and eligible students a reasonable window to opt out.
- ☐ Maintain documented procedures for parents and eligible students to inspect, review, and request amendment of education records.
- ☐ Define "school official" and "legitimate educational interest" in the annual notice, and apply the direct-control and use-limitation conditions to any outsourced function.
- ☐ Record each request for and disclosure of personally identifiable information, and keep that record with the education record.
- ☐ Use reasonable methods to authenticate the identity of any party before disclosing education records.

AUTHORITY 20 U.S.C. § 1232g · 34 CFR Part 99 (FERPA)

EdTech Vendor & Data-Privacy Agreements

California writes the rules of the road into every contract that touches pupil data.

- ☐ Execute a written agreement with every provider of digital storage, management, or retrieval of pupil records, or of educational software that handles pupil data.
- ☐ State that pupil records remain the property of and under the control of the local educational agency.
- ☐ Prohibit the provider from using pupil personally identifiable information for targeted advertising and from selling pupil data.
- ☐ Require a description of the provider's security and confidentiality measures and its breach-notification procedures.
- ☐ Require deletion or return of pupil records at the end of the contract, except records a student elects to retain in a personal account.
- ☐ Track every agreement against a current inventory of EdTech tools and SaaS applications that touch student data.

AUTHORITY Cal. Education Code § 49073.1 (AB 1584) · Cal. B&P Code § 22584 (SOPIPA)

Information Security Program (GLBA Safeguards)

If you disburse federal student aid, the FTC Safeguards Rule is now your audited baseline.

- ☐ Designate a Qualified Individual responsible for the written information security program.
- ☐ Maintain a written program of administrative, technical, and physical safeguards scaled to size and complexity.
- ☐ Conduct and document a written risk assessment, and reassess it on material change.
- ☐ Encrypt customer information in transit and at rest, or document Qualified-Individual-approved compensating controls.
- ☐ Maintain a written incident response plan and deliver an annual written report to a board or senior officer.
- ☐ Oversee service providers by contract and assess them periodically.

AUTHORITY 16 CFR Part 314 (FTC Safeguards Rule) · ED Title IV PPA / SAIG Agreement

Authentication & Access Controls

Multi-factor for anyone who can reach student or aid data, with least privilege behind it.

- ☐ Enforce multi-factor authentication for access to systems holding student, financial-aid, or employee records, including remote and administrator access.
- ☐ Apply least-privilege, role-based access and recertify entitlements at least annually for sensitive systems.
- ☐ Maintain a current inventory of access points, accounts, and authentication methods, and remove stale or excessive access.
- ☐ Implement and periodically test logging and monitoring sufficient to detect unauthorized access or tampering.
- ☐ Apply session time-outs, system hardening, and network segmentation around sensitive data stores.

AUTHORITY 16 CFR § 314.4(c) · FERPA reasonable methods · K12 SIX (Protect Identities)

Internet Safety & CIPA (E-Rate)

The conditions every E-Rate and federally funded device program must certify.

- ☐ Adopt a written internet safety policy addressing minors' access to inappropriate matter, safety in electronic communications, hacking, disclosure of minors' personal information, and harmful materials.
- ☐ Operate a technology protection measure that blocks or filters obscene matter, child pornography, and content harmful to minors.
- ☐ Monitor the online activity of minors as part of the internet safety policy.
- ☐ Provide reasonable public notice and hold at least one public hearing before adopting the policy.
- ☐ Educate minors on appropriate online behavior, social-networking and chat-room interaction, and

cyberbullying awareness and response.

AUTHORITY 47 U.S.C. § 254(h) · 47 CFR § 54.520 (CIPA) · Protecting Children in the 21st Century Act

Breach Notification & Incident Response

Several clocks start the moment a breach is reasonably suspected. Know all of them.

- ☐ Maintain a documented incident response program covering detection, assessment, containment, recovery, and post-incident review.
- ☐ Notify affected California residents of a breach of unencrypted personal information in the most expedient time possible and without unreasonable delay.
- ☐ Include in notices the incident description, data elements involved, toll-free contacts, and guidance on credit reports and fraud alerts.
- ☐ For Title IV institutions, report actual or suspected breaches to Federal Student Aid the day they are detected or suspected.
- ☐ For Title IV institutions, notify the FTC within 30 days of a notification event involving the unencrypted information of 500 or more individuals.
- ☐ Require contracts to obligate providers to notify the institution of incidents within a window that supports these deadlines.

AUTHORITY Cal. Civ. Code §§ 1798.29, 1798.82 · 16 CFR § 314.4(j) · ED/FSA SAIG breach reporting

Records Retention, Access & Disposal

Keep what the state requires, dispose of the rest securely, and notice the programs that watch students.

- ☐ Retain and classify mandatory, permanent, and other pupil records per the California records-retention schedule.
- ☐ Securely dispose of records containing personal information so they cannot be read or reconstructed.
- ☐ Before adopting any program to gather or maintain pupil information from social media, notify pupils and parents and provide a public-comment opportunity at a public meeting.
- ☐ Honor parent and eligible-student rights to access and challenge the content of pupil records within statutory timelines.
- ☐ Limit and log disclosures of pupil records to the categories California law permits.

AUTHORITY Cal. Education Code §§ 49073.6, 49060–49079 · 5 CCR §§ 16020–16027

Governance, Training & Review Readiness

Make the program defensible: trained people, board-level ownership, and findings closed on a clock.

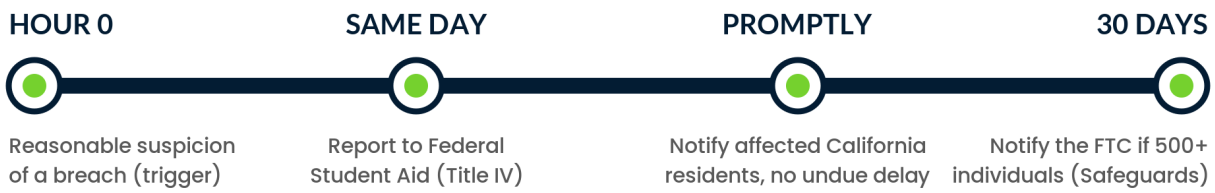
- ☐ Provide role-appropriate security and privacy awareness training to all staff, and maintain an acceptable-use policy.
- ☐ Obtain board or trustee approval of security and privacy policies, and review them at least annually.
- ☐ Report at least annually to the board or trustees on program status, incidents, and vendor posture.
- ☐ Track and remediate prior audit, program-review, and E-Rate findings with documented owners and timelines.
- ☐ Maintain evidence (policies, logs, training records, contracts) organized for FERPA, GLBA, CIPA, and California audits.

AUTHORITY 16 CFR § 314.4(e)–(i) · Cal. Education Code board-policy provisions · CDE / CCC guidance

INCIDENT CLOCK

When a breach is suspected, these clocks start

One trigger. Several deadlines. All running at the same time.



THROUGHOUT Contain, preserve evidence, recover, and run a documented post-incident review.

PART II · BEYOND COMPLIANCE

Where the next review cycle is headed.

Seven cards on the controls regulators and insurers do not all require yet, but that California schools and colleges are losing money and downtime to right now.

These items map to the threats the education sector reported losses on in 2024 and 2025: ransomware and extortion, AI-enabled and synthetic-identity fraud, financial-aid fraud rings, and EdTech supply-chain compromise. Treat unchecked items here as your strategic roadmap; the next review cycle is increasingly going to ask about them.

STRATEGIC ROADMAP

Seven forward-looking domains. 35 actions, mapped to where auditors, examiners, and insurers are heading next.

THREAT LANDSCAPE · 2024–2025

What the sector is losing to

Why the next review cycle is moving beyond compliance.

3.9M	+27%	$90M	150K
Student records exposed in confirmed U.S. education attacks (2025)	Year-over-year rise in exposed records	Federal student-aid losses to ineligible or synthetic applicants	Suspect identities flagged in federal student-aid forms (2025)

WHERE THE LOSSES COME FROM

- **Ransomware & extortion**
- **AI & synthetic-identity fraud**
- **Financial-aid fraud rings**
- **EdTech supply-chain compromise**

Sources: industry ransomware/breach trackers (2025); U.S. Dept. of Education / Federal Student Aid (2025).

Phishing-Resistant Identity & Zero Trust

Traditional MFA is now phishable. Move privileged accounts to FIDO2.

- ☐ Deploy phishing-resistant MFA (FIDO2 keys or device-bound passkeys) for administrators of the SIS, finance, identity, and email; retire SMS and one-time-code factors for high-risk roles.
- ☐ Eliminate standing administrative rights; grant just-in-time, just-enough access for privileged sessions.
- ☐ Implement privileged access management with credential vaulting, session recording, and automated rotation.
- ☐ Document a zero-trust roadmap with milestones across identity, device, network, and application pillars.
- ☐ Require step-up authentication based on device posture, location, and risk for sensitive transactions.

AUTHORITY CISA Phishing-Resistant MFA guidance · NIST SP 800-207 (Zero Trust)

Ransomware Resilience

Backups have to be immutable and tested. Counsel has to be at the tabletop.

- ☐ Implement the 3-2-1-1-0 backup rule: 3 copies, 2 media, 1 offsite, 1 immutable or air-gapped, 0 errors on restore tests.
- ☐ Maintain at least one immutable, logically air-gapped backup of the SIS, finance, and identity systems, tested quarterly for full restore.
- ☐ Maintain a ransomware-specific playbook covering containment, regulator and FSA notification, family and student communication, and ransom-decision authority.
- ☐ Conduct a full-scope ransomware tabletop annually, including cabinet, IT, communications, and outside counsel.
- ☐ Segment student, staff, building-systems, and backup networks; verify with periodic traffic-flow review.

AUTHORITY CISA #StopRansomware · K12 SIX Essentials (Backup & Restore Testing)

AI-Era & Synthetic-Identity Fraud Defense

Financial-aid fraud rings and deepfakes now target the admissions and business office.

- ☐ Deploy controls to detect synthetic and “ghost” students across admissions, enrollment, and financial-aid workflows.
- ☐ Require out-of-band callback verification for payment, payroll, vendor-bank-change, and refund requests above a defined threshold.
- ☐ Train admissions, financial-aid, HR, and finance staff on deepfake, voice-clone, and AI-phishing scenarios.
- ☐ Publish an AI acceptable-use policy covering approved tools, prohibited data (student PII and records), and

human-in-the-loop review.

- ☐ Review AI features in EdTech and business tools for data use and prompt-injection exposure before deployment.

AUTHORITY U.S. Dept. of Education / Federal Student Aid fraud alerts (2025) · NIST AI RMF 1.0

EdTech Supply Chain & SaaS Security

SOC 2 reports were never enough. Watch the apps and tokens continuously.

- ☐ Deploy SaaS Security Posture Management for Microsoft 365, Google Workspace, the SIS, and the LMS, covering OAuth tokens and third-party app permissions.
- ☐ Govern third-party app and integration approvals; review and revoke unused or over-permissioned OAuth grants.
- ☐ Subscribe to continuous vendor monitoring (security ratings and breach feeds) rather than annual questionnaires alone.
- ☐ Request an SBOM or equivalent component disclosure from critical software vendors, and re-request on major releases.
- ☐ Map fourth-party dependencies and concentration risk for the top critical vendors (SIS, identity, finance, hosting).

AUTHORITY CISA SBOM guidance · NIST SP 800-161 (Supply Chain Risk Management)

Email, Web & Network Hardening

The K12 SIX baseline your cyber-insurer now prices against.

- ☐ Enforce DMARC at p=reject with aligned SPF and DKIM on all sending domains.
- ☐ Defend against phishing and email-borne malware with advanced email filtering and user reporting.
- ☐ Deploy endpoint detection and response with tamper protection that end users cannot disable.
- ☐ Segment and limit student traffic and exposed services; filter malicious web content via DNS or proxy.
- ☐ Patch on a documented schedule and verify that automatic security updates remain enabled.

AUTHORITY K12 SIX Essential Cybersecurity Protections (2024-25) · CISA Cybersecurity Performance Goals

Threat Intel, Monitoring & Cloud Posture

Advisories feeding a 24/7 SOC, with cloud and recovery posture measured.

- ☐ Maintain MS-ISAC membership (and REN-ISAC for higher education); route advisories into a monitored workflow.
- ☐ Operate 24/7 monitoring with defined triage and escalation, in-house or through a managed SOC.
- ☐ Procure dark-web monitoring for institutional domains and employee credentials; feed hits into response runbooks.
- ☐ Deploy cloud security posture management across all tenants with continuous misconfiguration scanning.
- ☐ Define, document, and test RTO/RPO targets for tier-one services, and run a live failover or restore drill annually.

AUTHORITY CIS / MS-ISAC · REN-ISAC (higher education) · CISA KEV Catalog

Governance, Awareness & Board/Trustee Cyber Literacy

The board has to ask better questions. IT has to answer them with data.

- ☐ Run security-awareness training and recurring phishing simulations for all staff, with results tracked over time.
- ☐ Provide annual cyber-risk education to board members and trustees covering current threats and institutional obligations.
- ☐ Add a recurring cybersecurity agenda item with a KRI dashboard (MFA coverage, patch latency, phishing-fail rate, vendor risk).
- ☐ Maintain an insider-risk process with enhanced monitoring of departing employees and high-privilege accounts.
- ☐ Maintain a tested crisis-communications plan for families, students, staff, media, and regulators.

AUTHORITY CISA "Protecting Our Future: Cybersecurity for K-12" · NIST CSF 2.0 (Govern)

READINESS SCORE

PART I · REGULATORY	PART II · BEYOND COMPLIANCE
_____ / 44	_____ / 35

Next reassessment scheduled: _____

PART III · REFERENCES

Authority & further reading.

Every requirement in Part I traces to one of the documents below. Citations are intended for use in audit and program-review workpapers.

Primary Laws & Regulations

- 20 U.S.C. § 1232g; 34 CFR Part 99, Family Educational Rights and Privacy Act (FERPA)
- 47 U.S.C. § 254(h); 47 CFR § 54.520, Children's Internet Protection Act (CIPA)
- 16 CFR Part 314, FTC Safeguards Rule (Gramm-Leach-Bliley Act)
- Cal. Education Code § 49073.1, Pupil Records: Digital Storage & Education Software (AB 1584)
- Cal. Education Code §§ 49073.6 and 49060–49079, Privacy of Pupil Records
- Cal. Business & Professions Code § 22584, Student Online Personal Information Protection Act (SOPIPA)
- Cal. Civil Code §§ 1798.29 and 1798.82, Data Breach Notification

Federal & State Guidance

- U.S. Dept. of Education, Student Privacy Policy Office (PTAC) Guidance
- Federal Student Aid, GLBA / Safeguards Rule & SAIG Breach Reporting (Title IV)
- California Dept. of Education, Data Privacy & Security Guidance
- California Attorney General, "Ready for School" Student Privacy Guidance
- CCC Chancellor's Office, Information Security Standard (community colleges)

Frameworks, CISA & ISACs

- K12 SIX, Essential Cybersecurity Protections (2024-25)
- CISA, Protecting Our Future: Cybersecurity for K-12 & Cybersecurity Performance Goals
- NIST CSF 2.0 · NIST SP 800-207 (Zero Trust) · NIST AI RMF 1.0
- Center for Internet Security / MS-ISAC; REN-ISAC (higher education)
- CISA, Phishing-Resistant MFA & #StopRansomware guidance