Policies, People, and Protective Measures: Legal Requirements for K-12 Cybersecurity

Cybersecurity has become an increasingly pressing issue in K-12 education, as incidents have continued to escalate in frequency and severity. Responses to K-12 cyber attacks have focused on providing resources to educational institutions, increasing coordination and information sharing, and enforcing legal obligations.

Some of the basic legal requirements for K-12 cybersecurity are summarized in this CDT brief, along with strategies for compliance and working with vendors and external partners. However, the law sets only the minimum requirements, and educational institutions should also consider additional best practices around data ethics, data governance, and technical implementation.

Basic Legal Requirements

Three laws or groups of laws have a widespread impact on K-12 cybersecurity: the Family Educational Rights and Privacy Act (**FERPA**); the Children's Online Privacy Protection Act (**COPPA**); and varying state laws. These are not the only legal requirements around K-12 cybersecurity, but are the most important.

FERPA

What is FERPA?

- Federal law passed in 1974 that applies to school districts and schools that receive funds from the U.S. Department of Education (ED).
- Provides parents and adult students with rights to access student education records, request their amendment, and consent to their disclosure.
- Includes a number of exceptions to the consent requirement, including for "school officials" and for audits, evaluations, and studies for specific educational purposes.

What does FERPA Say About Cybersecurity?

ED has interpreted FERPA's provisions to *imply* a cybersecurity requirement, as it prohibits schools from having "a policy or practice of permitting the release of education records . . . without the written consent" of the parent or eligible student. Additionally, some of FERPA's exceptions include specific security requirements, such as:

- The "*school official" exception* allows disclosures to teachers, contractors, and technology vendors, but requires schools to "use reasonable methods" to limit the data access of school officials, including "physical or technological access controls" and "administrative policy."
- Audits, evaluations, or studies also require "*reasonable methods*" to limit use of student data and ensure data is destroyed when no longer needed.

Finally, ED issued a letter to a school district that stated:

> *We interpret this prohibition to mean that an educational agency or institution must use physical, technological, administrative and other methods, including training, to protect education records in ways that are reasonable and appropriate to the circumstances in which the information or records are maintained.*

COPPA

What Is COPPA?

- Federal law passed in 1999 that applies to for-profit "operators" of online services that are "directed to children" under 13.
- Prohibits collecting, using, or sharing personal information from a child without verifiable parental consent; enforced by Federal Trade Commission (FTC).
- Schools may consent to the collection and use of children's personal information in the "educational context."

What Does COPPA Say About Cybersecurity?

Unlike FERPA, COPPA includes an express cybersecurity requirement, but it is very broad:

> *COPPA requires online services to "[e]stablish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children."*

Additionally, the Federal Trade Commission, the agency responsible for COPPA's enforcement, issued a **policy statement that clarifies** that "[e]ven absent a breach, COPPA-covered ed tech providers violate COPPA if they lack reasonable security." Additionally, the FTC has interpreted COPPA's cybersecurity requirements in case-by-case enforcement to include written security **policies and procedures, training personnel**, and utilizing standard **technical measures**.

Although COPPA does not apply to schools, it may apply to their technology contractors, and its cybersecurity requirements may be helpful for schools in developing agreements with their contractors.

State Student Privacy Laws

What Are State Student Privacy Laws?

- There are 140+ state student privacy laws, with some predating FERPA but most passed in the past decade, including some in recent months.
- The laws cover a variety of topics, including parents' and students' data rights, targeted advertising, contracts with vendors, and cybersecurity.

What Do State Laws Say About Cybersecurity?

The following are examples of states' approaches to K-12 cybersecurity:

- **California** requires local educational agencies to contractually mandate that vendors take "actions" to "ensure the security and confidentiality of pupil records" and to report "cyberattacks impacting more than 500 pupils or personnel."
- **Colorado** requires both "local education providers" and ed-tech contractors to have information protection or security programs.
- **Maryland** requires county boards of education to adopt "reasonable security procedures and practices that are appropriate to the nature" of the student data.
- **Pennsylvania** requires school districts to notify individuals in seven business days and the District Attorney in three days of breaches of unencrypted personal information.

Dimensions of Legal Compliance

Both ED and the FTC have interpreted FERPA and COPPA to require reasonable security policies and governance, training and supporting personnel, and protective technical measures. The compliance strategies in this next section reflect recommendations by ED and the FTC as well as other agencies that provide cybersecurity support, including the Cybersecurity and Infrastructure Security Agency (CISA), the National Institute of Standards and Technology (NIST), and the Multistate Information Sharing and Analysis Center (MS-ISAC).

Policies and Governance

Although the term "cybersecurity" might conjure thoughts of technical countermeasures, it is first an organizational practice. The vast majority of cybersecurity incidents occur due to human error, with one study finding that human error is the cause of or contributes to as many as 95% of incidents. Policies and governance can help address the critical human component of cybersecurity.

- Establish comprehensive data security and incident response policies:
  - » Approved by organizational leadership.
  - » Based on an institutional cybersecurity review of risks and organizational maturity, ideally aligned with the NIST Cybersecurity Framework.
  - » Defines goals and a vision for reporting, remediation, review, and feedback.
- Formulate a concrete plan consistent with data security and incident response policies:
  - » Identify and standardize responsible parties and timelines for initial response, notification, and reporting.
  - » Address most common attack vectors such as Remote Desktop Protocol and unique organizational risks.
  - » Include procedures for performing and testing backups for partial and full restorations.

Resources for Policies and Governance

CISA, Protecting Our Future. Provides a comprehensive view of the challenges facing K-12 cybersecurity, including high-priority, high-impact steps schools can take now.

ED, Data Breach Response Checklist. An actionable series of steps that schools can take now to respond effectively to data breaches.

NIST, Cybersecurity Framework Quick Start Guide. An accessible guide to building your institutional governance in alignment with NIST's standards for policies and governance.

MS-ISAC, Nationwide Cybersecurity Review. Provides a methodological assessment of the maturity of your organization's cybersecurity policies and governance.

Training and Supporting Personnel

Another step in mitigating human error and in responding to incidents is training that supports school personnel and the school community:

- Create a training and awareness campaign on all levels and for all staff, including organizational leadership, IT staff, educators, parents, students, and school operations.
- Training should cover awareness (how to spot a threat such as a phishing email) and ability (what to do when a threat is suspected).
- Training should be regular, substantive, tailored for local contexts (including state laws), and up-to-date.
- Update content periodically to provide reflections on "lessons learned," alerts regarding new developments, and "just-in-time" training.

Resources for Training and Supporting Personnel

ED, Data Security and Management Training. General guidance for establishing training programs for education audiences. The guidance addresses awareness vs. training, training all employees, identifying and reporting breaches, creating a culture of security, and delivery methods. Developed by Privacy Technical Assistance Center (PTAC).

ED, Addressing Adversarial and Human-Caused Threats. Library of resources related to cybersecurity and physical security for use in training and distribution to the school community. Developed by the Readiness and Emergency Management for Schools Technical Assistance Center (REMS-TAC).

Department of Homeland Security et al., School Safety.org. An additional library of training and educational resources from across multiple agencies.

Protective Technical Measures

Finally, both FERPA and COPPA require institutions to adopt reasonable technical measures to protect student data.

- Take a small number of high-priority steps:
  - » Encrypt data at rest and in transit.
  - » Implement multifactor authentication (MFA, also referred to as 2FA), possibly in conjunction with a single-sign on (SSO) solution and beginning with the most vulnerable systems.
  - » Patch known security flaws and install software security updates.
  - » Perform and test back-ups.
  - » Periodically check for personal information that is wrongly stored or incorrectly public facing.
- Implement CISA's Cross-Sector Cybersecurity Performance Goals (CPG), which are a comprehensive set of best practices across sectors, rated by impact and complexity:
  - » Adopt tools for detecting unsuccessful logins.
  - » Set (and enforce) policies regarding minimum password strength.
  - » Separate user and privileged accounts.
  - » Maintain and secure network logs.
  - » Implement transport layer security.
  - » Incident reporting.

Resources for Protective Technical Measures

CISA, Cross-Sector Cybersecurity Performance Goals. Comprehensive guidance to technical measures to protect data, categorized by impact and complexity; although the full guidance is important, the checklist provides an accessible menu of tools.

NIST, FIPS 199. NIST guidance from its Federal Information Processing Standards (FIPS) series that aids in identifying the risk levels faced by each of individual IT systems.

NIST, FIPS 200, SP 800-53, and SP 800-53B (Excel file). Additional resources from the FIPS and Special Public (SP) series, that identifies specific technical measures tailored to each IT system's risk profile; SP 800-53B is a rubric that associates specific technical measures with specific risk profiles.

Governing Vendors and Partners

The key to working with vendors and external partners is expressly mandating cyber requirements and making those requirements contractually enforceable. Governance and policies play a major role in ensuring that (1) agreements are entered into with vendors, and (2) those agreements appropriately structure their cybersecurity obligations.

FERPA includes the following requirements for governing contractors:

- Use "reasonable methods" to limit access for "school officials" to records for which they have a "legitimate educational interest."
- Use "reasonable methods" and written agreements to "authorized representatives" conducting audits or evaluations that limit uses of student data and protect it from further disclosure.
- ED has recommended specifying data use limitations and security requirements in written agreement with recipients of student data and to verify the existence of a sound data security plan.

Similarly, COPPA requires that contractors and their subcontractors be "capable of maintaining the confidentiality, security and integrity" of data and "provide assurances" that they will secure data.

Schools may wish to take the following steps to hold contractors accountable:

- Include cybersecurity requirements in the procurement process and in evaluating bids;
- Specify in service agreements security requirements and incident procedures, including prompt notification in the event of a breach or other security incident; and
- Ensure that access for vendors is limited to necessary data.

That governance does not have to occur at the school or school district level, but can occur at the state level or even across states. State-level governance can result not only in standardized procedures across school districts, but increased bargaining leverage to ask more of vendors — and hold them accountable.

Resources for Governing Vendors and Partners

ED, Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices. Guidance from PTAC describing best practices and legal requirements while working with online ed-tech contractors; many of which are applicable to other contractors.

ED, Protecting Student Privacy While Using Online Educational Services: Model Terms of Service. Clause-by-clause analysis of provisions often included in terms of service with contractors, including both exemplars and problematic clauses; aligned with the above guidance. Produced by PTAC.

ED, Guidance for Reasonable Methods and Written Agreements. Guidance from PTAC on drafting written agreements to comply with the requirements of FERPA's audit or evaluation exception, but with generally applicable best practices.

This is one in a series of information sheets designed by CDT's Equity in Civic Technology team to give practitioners inside public agencies clear, actionable guidance on how to most responsibly use technology in support of the communities they serve. More info: https://cdt.org/civic-tech-inventory.