CoSN
LEADING EDUCATION INNOVATION

Building a Trusted Learning Environment: Understanding the Data Security Practice

TRUSTED LEARNING ENVIRONMENT

The TLE Program is supported by lead partners:

AASA THE SCHOOL SUPERINTENDENTS ASSOCIATION

ASBO ASSOCIATION OF SCHOOL BUSINESS OFFICIALS INTERNATIONAL

ASCD LEARN. TEACH. LEAD.

Whether your school system is managing a distance learning program or is operating with students in the physical classroom, it is difficult to overstate the importance of a strong data security program in protecting student data privacy. The education sector has emerged as a known target for bad actors, and the diversity of devices, data, and the individuals accessing it all create inherent vulnerabilities. Developing and implementing a data security program is a significant undertaking, and it can be easy to lose sight of the basics that serve as foundational protections for school systems.

Data security is one of the 5 core practice areas of the CoSN Trusted Learning Environment (TLE) Seal Program. This guide provides a detailed explanation of the TLE Data Security Practice requirements.

WHY DATA SECURITY MATTERS

Data security focuses on helping to ensure the confidentiality, integrity, and availability of the data. It is a pillar of any data protection program. One need look no further than the daily headlines to understand not only how important it is to develop and maintain a strong data security program, but also what a complex and challenging proposition it is to accomplish that in a way that is responsive to the modern threat environment.

In creating a strong data security program, it's important to note that technology controls are not enough. Instead, it's necessary to view security holistically across the organization, encompassing physical, technical, and administrative controls that works in partnership with a larger data privacy program, inclusive of employee training.

> "Education continues to be plagued by errors, social engineering and inadequately secured email credentials."
>
> 2019 Verizon Data Breach Investigations Report

.

District technology leaders play a critical role in implementing student data security programs, often taking on the role of chief security officer. To succeed, they need ongoing education, training and resources, as well as the attention of their superintendents to support their work and elevate the importance of maintaining strong security across the school system.

The CoSN Trusted Learning Environment Seal Program recognizes the significant work required to create a district data security program, and the pivotal role of the data security practice in any holistic student data privacy program.

> **"Hope is not a strategy.**
> **The time to prepare for a security incident is today."**
>
> Dan Layton, Chief Technology Officer,
> TLE Seal Recipient Zionsville Community Schools

COSN TRUSTED LEARNING ENVIRONMENT DATA SECURITY PRACTICE

TLE SECURITY PRACTICES

The TLE program includes 7 specific requirements for a school system data security program. These are not all-inclusive, but are considered fundamental to any school system student data privacy program, and are required in order to qualify to receive the TLE Seal.

1. PUBLICLY AVAILABLE POLICIES. The school system website includes its data privacy and security policies and practices which are updated as-needed, but at least on an annual basis.

School systems are expected to have data privacy and security policies and practices that encompass federal and state legal requirements and district norms. These are not a restatement of laws and regulations, but a customized, detailed set of policies addressing specific facets of applicable laws, regulations and district requirements, combined with documented practices that illustrate the behavior employees are expected to follow in order to achieve the policy goals.

Policies and practices should be updated at least annually to ensure that they reflect current requirements, industry standards and district needs, as well as to ensure that the communication is clear.

When possible, policies and practices should also be publicly available via the school system website. This helps to provide parents and other community members with the critical information they need to understand the school system's data protection efforts. In turn, this transparency helps to build the trust needed to maintain strong, collaborative relationships with parents and gives them the confidence they need that the school system is taking the necessary steps to protect their children's data.

2. MINIMAL REQUIREMENTS. There is a rather extensive volume of policies and procedures that are fundamental to any school system. However, there are some basics of data protection that are universal. School systems must have data privacy and security procedures that include:

- Defined data retention periods for student records;
- Technical protocols for securing data in transit;
- Physical, technical and administrative safeguards for securing data at-rest;
- Controls limiting access to data.

These policies and procedures should address data regardless of the format. From online storage to paper files, whether stored in the cloud, in local devices or in other storage facilities on or off the premises, the data protection requirements should be documented.

3. DATA STORAGE. In addition to ensuring that data is maintained for minimally-required time periods, secured in transit and at rest, and that account provisioning controls are in place, it's

important to establish policies that document where data may be stored in order to remain properly protected.

Whether stored on local computers, mobile devices, portable storage devices, cloud file-sharing or other storage services, not all data may be properly protected on all devices. Requirements and restrictions must be established by policy. In addition, enforceable policies must be in place to establish the rules for how each type of storage device must be configured and used to help ensure maximum data protections.

4. RULE/ROLE-BASED ACCESS. School systems collect and store a vast array of student data, but not everyone in the organization needs or should have access to all of that data. Access to both data and technology systems should be limited to "need to know." There must be a legitimate educational interest in employee access to data that considers the minimally required data elements and technology systems necessary for the employee to properly perform their role.

The process for determining which employees may access which data and systems, how requests for access are approved, and the process for provisioning and revoking access should be well-documented.

5. INCIDENT RESPONSE COMMUNICATIONS. An incident response procedure is fundamental to any security program. In the event of a data security incident, communications – internal and external – are critically important and must be managed properly. Any incident response plan should include a process for communicating pertinent information about the incident to appropriate internal stakeholders, external stakeholders involved in any investigation, and to impacted individuals, parents and other community members in accordance with state laws and school system policies.

The incident response procedure should make clear who is responsible for communications, including ensuring that public notification is conducted in accordance with regulations, and how that is accomplished. Communications templates, to be customized in the event of an incident, are also recommended.

6. DISASTER RECOVERY. In the event of a security incident, service interruption or other unforeseen issues impacting system or premises availability, it's important to have a plan in place to remain operational. A business continuity and disaster recovery plan establishes the protocols for activating back-up systems, implementing distance learning protocols and ensuring the physical safety of employees and students to ensure that any disruption to operations are minimal.

The plan should be verified and tested regularly, on an established schedule that is documented in policy and procedure.

7. AUDIT. Data protection efforts must be examined continuously to ensure they are effective, up to date, and properly enforced. Regular audits of data privacy and security practices must be conducted in order to understand:

- Is the data protection program performing as needed and as expected?
- Are there gaps in protection, knowledge, or communications?
- What are the logical next steps to improve the data protection program?

Of course, no security program will be effective without robust employee training in place to build and maintain awareness of what good security practices look like, how to recognize common threats, and what behaviors can compromise the school system's security.

GETTING STARTED

CoSN and other trusted organizations make a variety of resources available to school system leaders to support their ongoing student data privacy education.

ADDITIONAL RESOURCES

CoSN's Empowered Superintendent Initiative:

Trusted Learning Environment: The Role of Leadership in Protecting Student Data Privacy

An overview of the CoSN Trusted Learning Environment Program.

The Importance of Cybersecurity

5 critical reasons why district tech leaders must make cybersecurity a priority.

CoSN Privacy Initiative:

Trusted Learning From The Ground Up: Fundamental Data Governance Policies and Procedures

Basic data privacy policies and procedures every district should have in place.

CoSN Cybersecurity Initiative:

Cybersecurity Readiness Self-Assessment

Assess your district's cybersecurity readiness with this self-assessment tool.

Federal Trade Commission

Start with Security

Apply lessons drawn from FTC enforcement on industry cybersecurity issues to your district with this simple guide.

About the CoSN Trusted Learning Environment Seal Program

The Trusted Learning Environment Seal Program is the nation's only data privacy seal for school systems, focused on building a culture of trust and transparency. The Trusted Learning Environment (TLE) Seal Program was developed by CoSN (the Consortium for School Networking), in collaboration with a diverse group of 28 school system leaders nationwide and with support from AASA, The School Superintendents Association, the Association of School Business Officials International (ASBO) and ASCD. The Program requires school systems to have implemented high standards for student data privacy protections around five core practice areas: Leadership, Business, Data Security, Professional Development and Classroom. School systems that meet the Program requirements will earn the TLE Seal, signifying their commitment to student data privacy to their community. TLE Seal recipients commit to high standards and continuous examination and advancement of their privacy practices.

About CoSN

The Consortium for School Networking (CoSN), the national association of school system technology leaders, believes that technology is an essential component of learning today, and is deeply committed to the use and distribution of technology in school systems. However, all technologies must be properly assessed for design and appropriateness in the modern classroom. Educators and companies alike must recognize and uphold their responsibilities to protect the privacy of student data. Working together, educators and the private sector serve millions of students by providing them with the rich digital learning experiences and access needed to succeed in college, work and life. That partnership is critical to ensuring that students will have the tools necessary for success in the 21st century.