School System Privacy Stakeholders • trustedlearning.org

While someone must be in charge, it takes everyone in the school system, working in alignment, to properly protect student data privacy. Here is a snapshot of the many different roles across a school system that have an impact on student data privacy.

As you review this, consider: what does each individual need to know to properly protect student data privacy? How can you best partner on the work of protecting student data privacy across your school system?

TRUSTED LEARNING ENVIRONMENT

The work of building a student data privacy program is not the responsibility of one person or even one team. It takes everyone.

Superintendent/Board Members
Responsible for the risks associated with not properly protecting student data and for supporting development and implementation of the district privacy program. This includes responsibility for establishing student data privacy as a district priority and ensuring sufficient funding, spearheading development of critical privacy policies, making risk-based decisions, and ensuring that all stakeholders understand their privacy responsibilities.

Principals
Responsible for implementing district privacy policies and procedures, and ensuring that their building staff understand how to protect student data privacy in compliance with applicable laws and district requirements. Act as role models for their staff and students on protecting student data privacy.

Guidance Counselors
Have access to a wide range of student personal information, including grades, test scores, future plans, attitudes, aptitudes, financial needs, and recommendations. Require training on federal and state laws, district policies, and the actions they need to take to properly protect student data privacy.

Technology Leaders
Responsible for developing and implementing the district's student data privacy and security programs. Provide the expertise to translate policy into practice, and are responsible for everything from ensuring proper network configurations, setting access controls, responding to data security incidents, vetting classroom technologies, providing training, and more.

Teachers
Have access to a wide range of student data, and make decisions about their students' privacy every day, with each piece of classroom technology they use. Require training on federal and state laws, district policies, and the actions they need to take to properly protect student data privacy. Must ensure that they follow the school system vetting process before using classroom technologies. Must be able to explain to parents the benefits of the technology program and how student data privacy is protected, and model good privacy behaviors for their students.

Administrative Support/ Front Office Staff
Often have access to some of the most sensitive student data, such as family income, custodial relationships, citizenship and more, a privilege they are provided with in supporting school system leaders. Require training on federal and state laws, district policies, and the actions they need to take to properly protect student data privacy.

Instructional Materials Specialists
May have access to both de-identified student data as well as sensitive information to support fulfillment of individual education plans or to meet accommodations. Require training on federal and state laws, district policies, and the actions they need to take to properly protect student data privacy.

Assessment Coordinators
May have access to a wide range of sensitive student data, including grades, test scores, attitudes, and aptitudes. Require training on federal and state laws, district policies, and the actions they need to take to properly protect student data privacy.

Athletic Directors/Coaching Staff
Often have access to sensitive student personal information, including grades, behavioral data, and some health data. Require training on federal and state laws, district policies, and the actions they need to take to properly protect student data privacy.

School Health Professionals
Have access to sensitive student personal information in the form of health data, covering mental, physical, and emotional health, as well as medications and certain health exams. Require training on applicable laws, including on the intersection between the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Protection Act (HIPAA).

Records Management Officials
Often has access to a wide range of student personal information, encompassing the full education record, including transcripts. Require training on federal and state laws, district policies, and the actions they need to take to properly protect student data privacy, including strict protocols that define when records may be accessed and where they may be shared.

CoSN
LEADING EDUCATION INNOVATION

TRUSTED LEARNING ENVIRONMENT

More School System Privacy Stakeholders

trustedlearning.org

Procurement/Finance Officials

School business officials' privacy responsibilities include helping to coordinate vetting of school system technologies as part of the procurement process, in conjunction with technology leaders. Require training to understand federal and state legal requirements and district policies in order to help implement proper data protection agreements with third party service providers.

Academic Researchers

Often working with student information to perform longitudinal research, and may be sharing the data with partner organizations. Require training on the research provisions of federal and state laws, rigorous, industry-standard de-identification protocols, and human subject research protocols. Must also collaborate with technology and procurement teams to ensure that any technologies they plan to use have been properly vetted and that data protection agreements are in place with partners who may access student data.

Transportation Officials

Have access to student names, addresses, and schedules, as well as some behavioral data in order to coordinate the safe transport of students. Require training on safe use, handling, and destruction of the data they must access in order to provide their services.

School Safety Officers/ School Resource Officers

Must have access to sensitive personal information related to behavior – including suspected or confirmed criminal activity. Require training on the law enforcement and juvenile justice provisions of FERPA and state laws. Most work closely with district leadership to ensure their access to and use of student data is limited to what is necessary to provide for student safety in a manner that is consistent with district policies and community norms.

Food Service Providers

Often have access to student dietary restrictions and behaviors. In addition, some food service administrators may have access to aggregated, de-identified data related to free and reduced lunch status. Require training on federal laws, including the National Student Lunch Act, state laws, district policies, and the actions they need to take to properly protect student data privacy.

Vendors/Technology Providers

Often have access to student personal information in order to provide their services. Must understand and operate in compliance with all applicable federal and state privacy laws, have robust data privacy and security programs, and work in partnership with – and, as school officials – under the direct control of school systems to protect student data privacy.

Foundations/PTAs/Booster Clubs/Community Organizations

May operate independently as affiliated partners, and may receive a limited amount of student personal information in order to support students. Must understand and operate in compliance with all applicable federal and state privacy laws, have robust data privacy and security programs, and work in partnership with and under contract with school systems to protect student data privacy.

Community and Media Relations Officials

Responsible for crafting community and media messages in the event of a data security incident and to explain the benefits of the school system's technology program and use of student data to achieve educational outcomes. Must understand fundamentals of student data privacy requirements to support their work.

Parents

Have a special responsibility to understand and help enforce school system acceptable use policies to ensure proper and secure use of classroom technologies. Should be informed about how student data may be used to support their children, the benefits of the school system technology program, and how student data privacy is protected. Should be provided with student data privacy training and have a venue through which they can have their privacy questions answered.

Campus Planners

Often responsible for campus resource planning, and may have access to student population metrics, including enrollment trends. These teams do not normally require access to student personal information, but may need to be provided with training on industry standard de-identification protocols.

Facilities/Building/ Grounds Officials

Often responsible for system-wide infrastructure, such as HVAC systems. To the extent that these services are run on the school system network, they must work in close coordination with and heed the guidance of technology leaders to ensure that their work is done in a manner that maintains the security of the infrastructure.

Grant Officers

May be responsible for sending aggregated, de-identified data to grant providers to demonstrate efficacy of a grant-funded program. Need to work closely with technology leaders and procurement officers to ensure that their intended use of student data complies with legal requirements and district policies, and to implement proper contracts with partners to address sharing and use of de-identified data.

Students

Are responsible for their compliance with the school system acceptable use policy. Should also be provided with age-appropriate lessons on the fundamentals of data privacy, as well as online safety and digital citizenship.

CoSN

LEADING EDUCATION INNOVATION

About the CoSN Trusted Learning Environment Seal Program

trustedlearning.org

The Trusted Learning Environment Seal Program is the nation's only data privacy framework 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 also commit to continuous examination and demonstrable future advancement of their privacy practices.

The TLE Program is supported by lead partners:

AASA THE SCHOOL SUPERINTENDENTS ASSOCIATION

ASBO ASSOCIATION OF SCHOOL BUSINESS OFFICIALS INTERNATIONAL

ASCD®

For more information, visit trustedlearning.org or contact us at lattai@cosn.org.