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?

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 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.

Principals
- 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.

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.

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.

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.

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).

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.

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.

Teacher
- 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.

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.

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.

Instructional Leaders
- Spearheading development of critical privacy policies, making risk-based decisions, and ensuring that their building staff understand their privacy responsibilities.

School System Privacy Stakeholders • trustedlearning.org
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:

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