Student Data Privacy

A SCHOOL SYSTEM PRIORITY. AN ESSENTIAL COMMITMENT.

―――――

As citizens, students, educators, parents, employees, and consumers, we all have concerns about maintaining the privacy of our personal data. For school school systems, data privacy is a multi-stakeholder priority, and it touches every aspect of operations—from student transportation to instruction, assessment to athletics, and counseling to community initiatives. Today and going forward, student data privacy policies and their implementation are hard-wired for governance, discipline, purchasing, and communications processes. Assessing privacy and compliance policies and practices related to your system-wide use of technology is a continual priority.

FIVE CRITICAL GUIDELINES for ensuring data privacy in your use of technology

1 • Stay current and compliant with federal and state laws.

Working with your school system's legal counsel and coordinating compliance with your technology, assessment, curriculum, student services, human resources, and all technology vendors, is the first priority. While technology programs, employee behavior, and products and services are key components in compliance, the mandate begins at the school system's executive level. Many school systems designate a single senior leader or leadership team to ensure legal compliance and currency.

2 • Address community and stakeholder expectations early and often.

Provide a clear review of your data privacy policy and compliance practices on your website, student handbook, parent communications, staff policies, vendor documents, etc. At the same time, ask stakeholders about their expectations for data privacy and take those concerns into consideration when developing your policy. Communications and clarity go a long way in preventing issues, mitigating confusion, and in some cases, protecting against potential legal challenges.

3 • Keep instructional impacts in the picture.

Student data is essential in supporting learning and success. Data enhances continuous academic improvement and the power to personalize learning. The challenge is balancing instructional needs and opportunities with the need for privacy. Students, families, educators, school leaders, and vendors alike, all play a role in striking the appropriate balance between access to learning resources and services, and privacy.

4 • Responsive, responsible privacy administration and management mitigates RISK.

Continual management of a compliance program that designates rules, procedures, and appointing an individual or group responsible for decisions is a starting point. The Student Data Principles, created by CoSN and the Data Quality Campaign offer 10 critical guidelines to serve as the foundation of administration and management practices.

5 • Training. Training. Training.

Anyone who collects or has access to students' personal information needs and deserves training and resources. From the swimming coach to school bus driver, school librarian to the nurse, teachers, counselors, and administrators in every department...everyone should learn how to use student data securely, effectively, legally, and ethically, in keeping with your school system's policies and requirements.

Student data privacy is a long-standing area of CoSN engagement, expertise, and experience. You can access CoSN's comprehensive portfolio of resources at **CoSN.org/privacy** and **TrustedLearning.org**.

CoSN
LEADING EDUCATION INNOVATION

AASA
THE SCHOOL SUPERINTENDENTS ASSOCIATION

▶ LEARN MORE at **cosn.org**