Data Privacy and Security Don't Take a Spring Break: A Relatable Rubric for School Leaders as the School Year Races Toward Summer

April 30, 2025

By: Alfred Brunetti

Springtime has finally arrived. School districts are squarely in the grip of that familiar blur where Spring Break is behind us and the rush of end-of-year festivities, field trips, and final commencement preparations is in full effect. With this flurry of activity, it is understandable how complex concerns like data management and digital security could take a backseat; however, constant vigilance in these areas -- for the remainder of this school year and for all those to come -- are leadership priorities that cannot be forgotten. Traditionally, to fulfill their role as stewards of their students' privacy, school leaders only needed to be sure to not run afoul of long-standing federal laws like the Family Educational Rights and Privacy Act (FERPA) and the Children's Online Privacy Protection Act (COPPA), but the landscape has changed drastically.

Now, with a substantive update to COPPA which will come into effect this summer, the proliferation of state comprehensive data privacy laws and data breach laws applicable to the education space and the unstoppable wave of technological development and Artificial Intelligence-fueled innovations, a once short list of concerns, has grown exponentially. In addition to the primary function of making sure their students receive an excellent education, today's school leaders are confronted with the dynamic challenges of enabling student engagement and learning in an increasingly digital environment while ensuring the personal information of students and staff alike remains safeguarded and secure. One way to face this challenge head-on is to apply a framework recognizable to all educators: a traditional rubric.

The following data privacy-infused format ties important data governance objectives to performance levels that can serve as a platform from which school leaders and administrators can reflect, measure, and take action.

Criteria	Excellent (4)	Satisfactor
1. Data Mapping	You have a comprehensive data map covering all systems, student/staff data types, storage locations, and access roles; updated regularly	You have a map that inc systems an types; upda

You need to know what data you have, where it lives, and how it flows before you can use it and protect it effectively.

2. Investigating Privacy Practices	Regular audits and gap analyses of operations and controls are performed and documented; policies are regularly reviewed and updated; new laws and guidelines are monitored and incorporated	An audit of and control performed, and genera with laws; r occasionall

Do your current practices and policies reflect today's legal, cultural, and ethical standards? There's no way to know unless you investigate and document at a regular cadence.

3. Vendor & EdTech Assessment	Thorough and documented vetting of all vendors against an established protocol; contracts include strong data protection terms; risk assessments documented	Vendor agr include bas protection v some revie practices

Vet your tools like you would vet a curriculum. An educator would not be allowed to teach without undergoing an interview process and satisfying ongoing supervision. EdTech tools often serve as both a tool and as an educator so be sure slick interfaces and catchy design features don't prevent you from digging into and understanding what they do with the data entrusted to you.

4. Ongoing Monitoring	Continuous monitoring system in place; incidents tracked and used to improve practices; audits conducted	Periodic ch reviews occ addressed

Data privacy and information security are not set-it-and-forget-it obligations. Data flows and practices are living organisms which need to be tracked and regularly reassessed.

5. Staff & Student Training	Mandatory, role-based training provided annually; content updated with legal/tech changes	Annual train but general specific

Even a perfectly written policy or protocol is worthless unless staff and students understand it and place it into practice.

By remaining mindful of these steps, school leaders can create a privacy-forward and digitally responsible culture in which their students and staff can feel secure and thrive.