Data Security Advice for K–12 Leaders

It is increasingly important for schools and districts to understand data protection and cybersecurity, yet many school leaders struggle to understand what actions are required and how to comply with new legal requirements. School faculty need the knowledge and skills necessary to strengthen security policies and procedures.

According to the State of K-12 Security 2022 report, there have been a total of 1,331 publicly disclosed school cyber incidents affecting U.S. school districts (and other public educational organizations) since 2016. Averaged over the last six years, this equates to a rate of more than one K-12 cyber incident per school day being experienced by the nation's public schools. These security incidents include student data breaches, data breaches involving teachers and school community members, ransomware attacks, business email compromise (BEC) scams, denial of service (DoS) attacks, website and social media defacement, and online class and school meeting invasions.

In CoSN's EdTech Trends 2021 report, survey respondents ranked cybersecurity as their top unmet technology need. One respondent called the need for more cybersecurity funding as "desperate." Another respondent's comment addressed the inequities inherent in funding cybersecurity at the local level, "Cybersecurity needs to be provided as a minimum blanket coverage for schools. Minimum coverage should be considered at a state level, so all districts start with an equitable security standard."

Striking a Balance

Gallup reached a nationally representative sample of 3,210 teachers, 1,163 principals, 1,219 district administrators and 2,696 students. The result is Making Meaning of The 2019 New Schools-Gallup Survey of Educator & Student Perceptions of Ed Tech. The New Schools-Gallup survey showed that most educators are using ed tech and would like to use it even more. In fact, 65% of teachers are using digital learning tools to teach every day and 87% are using it at least a few days per week. That is a significant jump from just a few years ago. And while it is clear that student data enhances continuous academic improvement and the power to personalize learning, the appropriate balance must be struck between instructional needs and security.

To Err is Human

While the most valuable asset of a school is its people, staff and faculty can also be a school's principal weakness in terms of data security. Whether it's including the wrong attachment or clicking on a phishing email, human error can wreak havoc on a school's network. Ensuring that faculty only have access to the data that they absolutely need for their jobs is vital.

A solid data security strategy requires that security principles are embedded in everyday school life, rather than simply having staff be "up to date" on the latest security and privacy legislation. Everyone who has access to student data needs to learn how to handle this data securely, effectively, and ethically.

One approach in protecting data is to minimize the amount of it that a school has. Faculty should first

consider what data is absolutely necessary to collect, treating data like how one would treat hard copy files with limited filing space. Another consideration to removing human error is to deploy artificial intelligence. AI-powered content filtering tools not only help block students' access to harmful content but often include privacy features that can support the protection of sensitive information.

> **"A solid data security strategy requires that security principles are embedded in everyday school life."**

From the Top

Some administrators take a hands-off approach to cybersecurity, while many districts don't offer regular cybersecurity training to staff. But data security is not simply an IT problem: it's a multi-stakeholder priority for school districts that starts at the top. Superintendents are crucial to district cybersecurity efforts. They establish the issue as a priority, while ensuring that stakeholders (such as parents) are informed about the district's security program. One simple thing administrators can do is to ask questions about relevant procedures and what the current response is to data breaches or other cyber incidents.

A School-wide Effort

Faculty need to understand that cybersecurity affects all operations of school: everything from digital learning in the classroom and regulatory concerns such as FERPA to operations and even payroll.

To help with cybersecurity efforts, it's advisable to start with education and change management. This could take shape as, for example, requiring that IT vet any new applications that teachers wish to use in their classrooms. It can also take form as a thorough education into how "bad actors" can easily access faculty email accounts. School leaders should do whatever it takes to instill a school-wide respect for—and understanding of—data security.

Sending educators to education technology conferences to learn best practices and obtain information that they can later share with peers is another way to open minds to the threats at hand, as well as well as learning new measures to prevent cyberattacks. IT professionals and faculty can also work together on digital citizenship instruction for students.

Continual management of a compliance program that designates rules, procedures, and the individual or group responsible for decisions is a good starting point. Working with your district's legal counsel and coordinating compliance with your technology, assessment, curriculum, student services, human resources, and all technology vendors, should also be a priority.

Other Considerations

Student data policies are inextricably tied to governance, discipline, purchasing, and communications practices. School leaders should know that protecting student data privacy is a primary concern of parents and peers, and that no governance program can be effective without their support. Assessing privacy and compliance policies and practices is constantly top of mind: or should be. A school's data privacy and compliance practices should also be easily available on the school's website, student handbooks, and various communications.

If you consider the costs of stolen, damaged or compromised data—not to mention the cost of a school's reputation—it is clear that schools and districts can't afford to let down their guard when it comes to cybersecurity. It's an investment that will only pay off great dividends in the future.