Managing Data Security and Privacy Issues with Remote Learning Technology

By Souvanny Miller, Leila Javanshir, and David Rice
April 29, 2020

With the rapid spread of COVID-19, school districts are surging toward remote online learning programs. Remote learning technology and other forms of educational technology ("ed tech") allow districts to educate students while physical distancing requirements remain in place by providing access to learning materials, video instruction, grades, coursework, and instructor feedback. Ed tech also introduces privacy and data security concerns, however, and districts must ensure that they comply with legal requirements and best practices when providing remote learning opportunities.

Below is guidance on the most pressing privacy and data security issues facing districts:

1. Understand what information is being shared with remote learning vendors and what they are doing with it.

When districts use remote learning tools, they might share sensitive student information with technology companies. School districts should review vendor contract terms carefully because vendor collection and use practices can be surprising. Most remote communications technology was not developed for the education space and the specific sensitivities associated with it.

There have been government and industry warnings about the security practices of some vendors, so districts should research technologies before adopting them. In some cases, vendors offering "free" services may be monetizing collected student data in ways that conflict with a school's legal obligations. Not all remote learning technologies require the sharing of data; some programs do not require students to log in or provide personal information to participate.

In some cases, districts may be unable to revise undesirable contract terms. But if a district can make changes, it should amend its agreements so that vendors can collect and use data only as necessary to perform the contract.

2. Understand the legal implications of collecting and using children's personal information.

The Children's Online Privacy Protection Act (COPPA) requires commercial websites and online services to obtain verifiable parental consent before collecting personal information from children under 13. Although COPPA generally does not apply to educational institutions, districts need to understand COPPA obligations for the following reasons:

- Vendors engaged by districts to provide online learning must obtain parental consent if the vendors collect student data;
- Districts can consent to the collection of children's information on behalf of parents, but only in the educational context—vendors' collection of personal information from students for the use and benefit of the school; and

---

Disclaimer: This article is not legal advice. It is provided solely for informational and educational purposes and does not fully address the complexity of the issues or steps business must take under applicable laws.

- COPPA explains what vendors must do to keep children's information safe and what information they must provide districts for districts to properly consent to collection.

Institutions subject to the Federal Education Rights and Privacy Act (FERPA) have additional considerations. FERPA generally prohibits the unauthorized disclosure of personally identifiable information (PII) maintained in education records, unless a vendor:

- Provides a service that would otherwise be provided by a school employee;
- Meets the criteria for a school official with a "legitimate educational interest" in education records as set forth in the school's annual notification of FERPA rights;
- Is under the school's direct control with regard to the use and maintenance of education records; and
- Uses education records only for authorized purposes and will not redisclose PII from education records to third parties (which should be addressed in the district's contracts), unless otherwise appropriately authorized and permitted by FERPA.

Districts should review FERPA notices and policies as well as vendor contracts to determine whether revisions are necessary during this remote learning period.

3. Implement appropriate network safety.

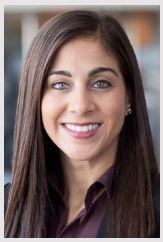
School employees' remote work also raises security issues. Employees must access sensitive information using their home networks and, in some cases, with their personal computers, which are less secure than the district's networks and equipment. When employees use personal devices, it becomes much more difficult to prevent, identify, and mitigate a data breach. Employees working remotely should be using a secure company computer system, a digital workspace platform (e.g., Citrix), or a remote connection through a secure virtual private network (VPN) to limit vulnerabilities.

Multifactor authentication, which requires users to enter at least two credentials to enter a network, is a strong step toward preventing attackers from gaining access. Additionally, reminding employees not to save personal or confidential information to their personal devices and asking them to review school policies are good ways for a district to get its team started on the right foot.

With a better understanding of risks and challenges involved in remote learning and ed tech generally, schools are well positioned to leverage the remarkable potential of these technologies and continue educating students.

Souvanny Miller is an associate on the firm's education team. She has experience advising municipalities and other public entities in regulatory compliance, constitutional law, and public records and public meetings law. Souvanny has also represented clients in administrative proceedings, in Oregon circuit courts, and before the Oregon Court of Appeals. She understands and appreciates how legal decisions and strategies will impact the goals of mission-driven public entities.

Direct: 503.205.2363 | **Email:** souvanny.miller@millernash.com



Leila Javanshir is a certified information privacy professional (CIPP-US) and a member of the firm's business practice. Leila began her career with the firm as a summer associate in 2017, assisting with matters involving privacy, data security, intellectual property, vendor contracting, and federal and state regulatory compliance. A significant part of Leila's practice includes providing privacy compliance advice and drafting consumer-facing privacy policies and terms that comply with applicable privacy and data protection frameworks.

Direct: 206.777.7437 | **Email:** leila.javanshir@millernash.com

David Rice, CIPP-US, provides strategic advice to clients on data privacy and security, data breaches, technology transactions, and cloud services and infrastructure. David was a pioneer in understanding the legal aspects of collecting, managing, storing, and protecting data. He has over twenty years of experience working with clients on data privacy and security matters.

Direct: 206.777.7424 | **Email:** david.rice@millernash.com