# A Data Protection Checklist for Education Vendors Navigating the "New Normal" of Remote Learning

*SmithAmundsen Data Privacy & Security Alert*
September 28, 2020

With the start of a new school year in the midst of a pandemic, many schools have opted to remain fully online or opted to have a hybrid learning environment. Regardless of the route school districts have chosen to take, the shift to online learning has opened educators' eyes to the many online tools available to them. In fact, the desire to incorporate online education platforms and tools will likely remain, even after life returns to "normal." As providers and third-party business partners together with educational institutions adjust to recent murkiness or uncertainty for online tools, it is important to keep in mind data privacy laws that impact the digital education space. Therefore, if you are operating in this cyber or digital space for the 2020-2021 school year, run through this compliance "checklist" first:

1. **Do you have proper consent? And how are you handling data collection?** Many online businesses may be familiar with the Children's Online Privacy Protection Act (COPPA) that requires companies to have a privacy policy, inform parents, and obtain parental consent in order to collect information from children. However, if schools are using websites, applications, or other tools for educational purposes, then teachers or school administrators may be the ones providing consent on behalf of parents. The caveat? Even with consent, companies can only collect student data that is used for an "educational purpose." As a result, beyond making sure you are recording proper consent, it is important to acknowledge that there are still data collection constraints once the consent has been granted.
2. **How are you storing student data?** When schools went fully remote at the start of the pandemic, there was a lot of concern around students being on camera. However from a privacy perspective the problem is not the act of being on camera, but rather the *storing* of footage. The Family Educational Rights and Privacy Act (FERPA) has strict guidelines regarding education records kept by schools and school districts. When a student's image, name, or voice is recorded and then stored by the school, this is when educators—and their platforms—may run into legal issues. The information collected about students while on camera is now a part of the institution's record and needs to be protected as such. From an educator's perspective, this means


**PROFESSIONALS**

Molly A. Arranz
Partner


**RELATED SERVICES**

Cybersecurity & Data Privacy

the students' information needs to be protected and accessible only to those allowed access under FERPA. If you are a vendor or business partner for a school and collecting and storing student information—written or recorded—it is important to ensure records will not only be securely stored, but also securely transferred to storage.

3. **Do you have to collect or store medical records?** While FERPA rules the roost on how educators must maintain records, all vendors that may have access to medical records, or are storing medical records, must still comply with HIPAA. With the rise in temperature checks, whether self-administered or via the school, there seems to be a misconception that temperatures could be a form of biometric data. Because legally-protected identification of an individual is not generally based on a temperature, it wouldn't be biometric data. However, it is still a medical record that must be properly protected; therefore, if your business is helping schools store these types of records it is important to ensure that they are properly secured.
4. **Are there any state laws to keep on your radar?** When it comes to education, while there are plenty of federal regulations about which vendors should be aware, there are also a host of state laws to be cognizant of as well. Some states specifically regulate education tech vendors; some states regulate local education agencies; and, some states regulate both. This is why it is important to always note where your client is located, or what states are part of your business relationship to ensure there are not additional state laws that impact your operation.
5. **Consider implications beyond your *legal* duty.** The current rise of data privacy concerns has left consumers, including parents and school administrators, wanting more transparency—especially when it comes to parents concerned about their child's data footprint. This is why some online education vendors, including Google, have committed to the Student Privacy Pledge created by the Future of Privacy Forum. While the pledge may not be legally required, consider joining this pledge and ensure you exercise good data hygiene. By having your company outwardly commit to safeguarding student information—whether through a formal pledge or via your own public facing statement—it shows consumers that you are cognizant of the heightened concerns around students' data.