

Managing COVID-19 Disruption: Key Student Privacy Requirements Remain Unchanged

March 23, 2020

As the nation seeks to respond and adapt to the COVID-19 pandemic, there have been widespread changes in the regulatory environment, particularly in the education sector. While quarantines and mandated closures of face-to-face instruction has required an increasing number of emergency waivers and changes in regulatory requirements, one area that has remained untouched is the protection of student privacy. As students of all ages urgently transition from a classroom to a virtual environment, concern over the protection of student privacy remains at a high level.

Often, this transition requires schools to turn to outside technology providers to support the development, implementation and maintenance of the online environment. This surge in demand for support extends beyond video conference services and online instruction to support for maintaining existing student financial aid, providing emergency assistance in higher education and offering special education support for children. Likewise, place-bounded programs are suddenly thrust into having students learning across state and national boundaries.

Many edtech companies have responded to these unprecedented challenges to expand the capacity and scope of their services. Radical changes in both the number of students served and the scope of services provided are placing extraordinary demands on institutions and providers alike. As these critically important efforts move forward, it is essential to be mindful of the variety of student data privacy laws that exist at the state, federal and transnational levels.

These laws generally break down into three buckets:

- Federal, notably the Family Educational Rights and Privacy Act and the Children's Online Privacy Protection Act
- State, such as California's Student Online Personal Information Protection Act
- International, most importantly the EU's General Data Protection Regulation

To date, there have been no waivers or modifications to these laws in response to the rapid build-out of online learning occasioned by the COVID-19 pandemic.

Technology companies offering solutions to schools should continue to ensure they have adequate operational, contractual and administrative safeguards in place to maintain compliance with student data privacy laws. This is particularly critical for companies that are primarily operating in an enterprise setting.

FERPA

FERPA requires all schools that receive any form of federal assistance (from K-12 through postsecondary) maintain control over personally identifiable information that are part of a student's educational record. Schools that allow companies to handle PII must have specific contractual provisions in their agreements, and contracting companies need to ensure the same thing among their subcontractors who have access to PII. It also requires vendors to have appropriate internal policies to be able to respond to parent or student requests to review data maintained about them. None of this is new, but with many companies greatly expanding their scope and volume of services, and with many new institutional clients, maintaining compliance with these requirements is all the more important.

Note that while the US Department of Education has not issued guidance specifically on this point, it has provided guidance on how schools can [share health and safety](#) related information in response to the COVID-19 pandemic.

COPPA

COPPA is enforced by the Federal Trade Commission and requires any online service intentionally collecting data from children under the age of 13 to first obtain verifiable parental consent. There is a [general exception](#) to this requirement for services provided under a contract with a school. In order to utilize this exception, vendors must ensure their agreements with schools, districts and states include appropriate language confirming that the client is in fact providing this consent consistent with its own policies including any appropriate parental notice.

State laws

Technology companies that have focused on K-12 schools as their primary customers know that navigating the patchwork of state student privacy laws is one of the biggest hurdles in managing district contracting. Unlike FERPA and COPPA, these typically require much more detailed contractual provisions, as well as operational adjustments regarding how data is used, maintained, stored and shared. The first and still the high water mark for these laws remains California's [SOPIPA](#).

As of this writing, the California Attorney General has not waived any requirements of SOPIPA for providers assisting schools in this rapid transition from classroom to online, nor based on the information available to us, have any other states done so at this time. It is essential that technology companies are knowledgeable about the risks and requirements of these laws, particularly as they are called upon to work with schools and districts across the country that may be far less experienced.

UK and EU operations – GDPR

In theory, the forced transition to online education may more broadly subject institutions to laws, such as GDPR, that may not have been prior focal points. There appears to be broad understanding among regulatory authorities that all organizations may need to prioritize other critical needs in the immediate term. A good-faith, pragmatic approach to protecting the privacy of students (and employees) will substantially reduce risk.

In response to the COVID-19 emergency in Europe, the European Data Protection Board has issued pragmatic privacy guidance while reminding organizations that GDPR's existing protections remain in place. Our cyber/data/privacy team's analysis of this guidance is [here](#).

Similarly, the UK's Information Commissioner's Office published guidance last week. Our analysis of that guidance is [here](#).

The Cooley [education](#) and [cyber/data/privacy](#) teams are closely monitoring this still-evolving situation.

Matt Johnson focuses on assisting higher education institutions and education technology companies regarding a variety of regulatory issues including state and federal privacy laws at the K-12 and postsecondary levels.

This content is provided for general informational purposes only, and your access or use of the content does not create an attorney-client relationship between you or your organization and Cooley LLP, Cooley (UK) LLP, or any other affiliated practice or entity (collectively referred to as "Cooley"). By accessing this content, you agree that the information provided does not constitute legal or other professional advice. This content is not a substitute for obtaining legal advice from a qualified attorney licensed in your jurisdiction, and you should not act or refrain from acting based on this content. This content may be changed without notice. It is not guaranteed to be complete, correct or up to date, and it may not reflect the most current legal developments. Prior results do not guarantee a similar outcome. Do not send any confidential information to Cooley, as we do not have any duty to keep any information you provide to us confidential. This content may have been generated with the assistance of artificial intelligence (AI) in accordance with our [AI Principles](#), may be considered Attorney Advertising and is subject to our [legal notices](#). Copyright © 2026