WHITEPAPER

How student security and privacy impact edtech applications

Clever

WHITEPAPER

Clever

How student security and privacy impact edtech applications

The material in this whitepaper is not legal advice and is intended to offer a broad-brush perspective. We encourage you to speak to your lawyer for advice specific to your product and team.

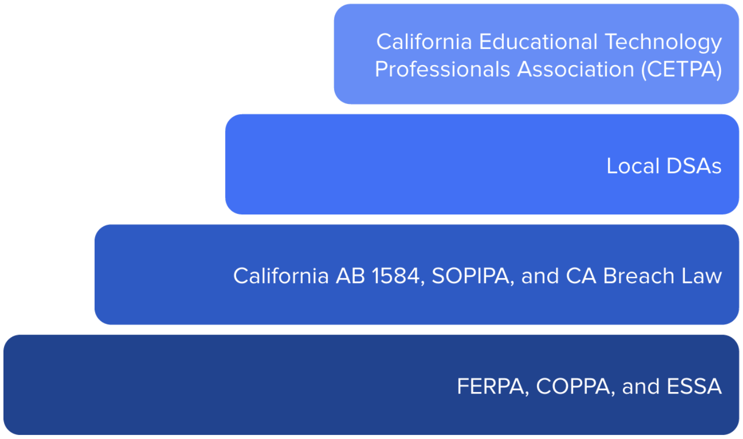
Internet privacy is on everyone’s mind these days, including legislators, free-speech activists, and pretty much anyone who shops online or voices an opinion in forums like Facebook. Privacy concerns have given rise to a dizzying array of legal agreements, disclaimers, and boilerplate policy statements. Indeed, researchers at Carnegie Mellon University published a study that estimated that it would take 76 workdays just to read all the privacy policies on the websites the average Internet user visits each year.

While some may ignore or breeze through the many privacy policies they encounter, others—such as software developers in the educational technology sector—don’t have that luxury. “As an edtech company, not only do you have to read every applicable law and contract, you also need to ensure that your company complies with the laws, regulations, and agreements pertaining to the privacy and security of student data,” says Alex Smolen, a security expert who led the account security team at Twitter and is now the lead security engineer at Clever. “It can be a time-consuming struggle—and for developers, it’s all time spent not building features or providing support.”

Case Study: California

A good illustration of the multi-layered and complex privacy and security regulations edtech developers have to deal with is the state of California—which Clever is well acquainted with, since it’s in about 70 percent of California’s school districts. Say you’ve got a brand new

The legal landscape


California Educational Technology Professionals Association (CETPA)
Local DSAs
California AB 1584, SOPIPA, and CA Breach Law
FERPA, COPPA, and ESSA

application you're hoping to roll out in some of California's districts. To begin with, you'll have to comply with the big three federal educational laws: the Family Educational Rights and Privacy Act (FERPA), the Child Online Privacy Protection Act (COPPA), and the Every Student Succeeds Act (ESSA). To do so, you need to address a host of questions. Do you have a way for parents to change student information within your system? Do you have a mechanism for deleting student data? And if the district asks, can you help the district fulfill a request to report on foster, homeless, or military youth?

Next, you'll have to layer on California's own laws governing student privacy. One of the most important ones came into effect in 2016: the Student Online Personal Information Protection Act (SOPIPA), which limits third-party advertising, among other things. Even though it's a California specific law. SOPIPA has had a big impact across the country, inspiring scores of copycat bills in other states.

Once you've complied with the federal and state requirements, you as an educational software vendor can legally work in California—but of course, you'll have to contract with different districts. You'll probably need to create request for proposals (RFPs) for a variety of districts, committing to meet their specific privacy and security requirements. It's also likely you'll need to work out multiple data-sharing agreements (DSAs) and memorandums of understanding (MOUs) with other districts. And each of those agreements may specify different breach-notification periods—one district might require parental notification within three hours of a breach discovery, another within five days, yet another within 60 days.

Last, but not least, you'll need to make sure you're in sync with local requirements and industry trends. Districts may enquire if you've signed the Student Privacy Pledge, and others might ask you to sign the California Common Contract put together by the California Educational Technology Professionals Association (CETPA).

After all that, you'll finally be a position to roll out your application to California classrooms—but you'll have to address the technological complexities that go along with doing business online.

Staying ahead of third-party tracking technology

One area of special concern for edtech developers is web trackers belonging to third parties such as advertisers. Website advertising trackers usually involve a single line of code that calls out to a third-party advertising network that collects usage data, aggregates it with other sites, and sells it. Because COPPA prohibits websites from collecting data from students under the age of 13 without parental consent, companies in the edtech sector need to be especially careful about the third-party scripts they include in their websites.

When it comes to third-party advertising trackers, noncompliance can be costly—not only in contracts lost, but also in hefty fines. The New York attorney general recently brought actions against major media companies for collecting information from children through tracking technologies without parental consent. Mattel and Viacom argued that their websites were directed at parents, not children, but they were unsuccessful in making that case. The attorney general's office decided that under COPPA, website operators must treat mixed audience pages as child-directed and remove third-party advertising tracking tools—and it issued fines of nearly $1,000,000.

Clever is vigilant about third-party tracking. "When our lawyer noticed that one of the scripts on the front page of clever.com was labeled as an advertising tracker by a popular privacy-enhancing browser plug-in, she suggested it might put the company at odds with COPPA," Smolen explains. After delving into the issue, Clever discovered that the script had been mislabeled; it was really a first-party analytics tracker that gathered data about user experiences to help improve them. "But to be cautious, Clever removed the script from our website and updated policies on third-party software scripts," he adds.

Clever's new approach is backed up by a technology called Content Security Policy that automatically blocks external scripts from loading unless they're specifically authorized. "The outcome is automated enforcement that complies with COPPA's terms on targeted advertising," Smolen points out.

Tips for applications grappling with privacy and security

Clever's lead security engineer, Alex Smolen, has some advice for educational software developers concerned about student privacy and security, whether they're rolling out their applications on their own or leveraging Clever's infrastructure and expertise.

Policies are important—as are the people who carry them out. "Perfect policy does not lead to perfect compliance—because policies by themselves are still just words on paper. People take the path of least resistance, and sometimes security and privacy isn't an employee's primary objective. Try to build a culture where people understand that security and privacy are so important that they should be everyone's job."

Enlist your engineers. "Having a documented process with logs for how policies are audited is a good start. The automation of key processes—for example, the process of onboarding employees or reviewing code for potential security issues—is even better. That means that engineering must be involved in, and ultimately responsible for, the process. Having engineering as a key stakeholder in privacy and security compliance is a sound practice."

Audits can be good for you. "Because security is adversarial in nature, it's important to get some fresh thinking about how your systems work—and how they work together. And I'd advise developers to regularly rotate the auditors you use. That way, you'll benefit from a range of approaches, including your resistance to different attack paths. But remember, audits have their limits. They can't be continuous, so they only provide a snapshot at one point in time. Meanwhile, code is ever evolving."

> Try to build a culture where people understand that security and privacy are so important, they should be everyone’s job.
>
> **Alex Smolen**

Bring in others to help squash your bugs. “To make audits more continuous, look into hosting a bug-bounty program. They allow you to reward external security people for finding issues with your software. And because bug hunts can happen continuously, they can increase how quickly you’re able to find security issues.”

Consider the cloud. “Storing data in the cloud dictates a shared responsibility model. There are certain security issues outside your responsibility. For instance, developers have to rely on auditing from their cloud providers. But other things remain your responsibility as a software developer, like the security of the configuration of your virtual networks. So one, understand the security of your cloud provider. And two, use best practices as you set up your cloud infrastructure.”

Steps for scaling security and privacy compliance

Because the requirements for student data security and privacy are so complex, compliance can be challenging for educational software developers. Which is why Clever uses a systematic approach—and automation—to tackle the core issues. “At Clever, data security and privacy are at the core of our company mission,” Smolen says. “We think about it with every change we make and every new feature we introduce.”

Here’s a quick overview of the steps Clever takes to ensure privacy and security compliance:

Map legal languages to controls

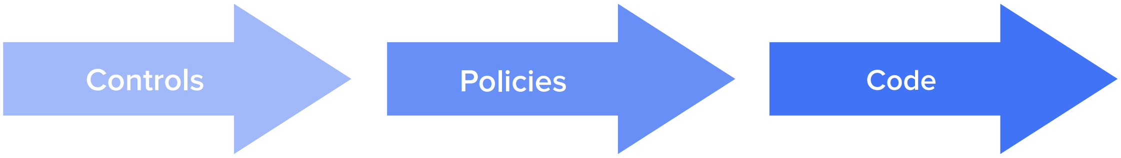
Define controls with policies

Automate policies with code

Stay informed about the changing regulatory landscape—and its implications for edtech. The first thing to do is to assess the laws to determine the procedural and technical controls that they reference. That process involves poring over a lot of legal material—and a lot of fine print—to determine the implications for software that’s used in the edtech space. “We then define (or reshape) our policies to comply with legal requirements,” Smolen says.

Map laws to controls. After Clever has identified aspects of a new law or contract that apply to student data privacy, it then attempts to map them to existing controls. If it identifies gaps, it addresses them. “Sometimes the law in question is more lax than our existing controls,” Smolen explains. “But if the law is more stringent, we may not have a control for the legal issue in question. In that case, we create a plan for addressing the gaps.” In some cases, that can be a difficult and expensive process. For instance, Clever’s project to encrypt all data at rest took several months of effort—but the company felt it was a critical investment to make.

Leverage automation. Once Clever understands the law and has identified its engineering priorities, it starts building automation to lessen the work involved in being compliant. “That way, we minimize both our legal risk and the effort we have to spend to stay compliant,” he says. “Automation is investment in the process.”



Steps for scaling compliance

Because Clever’s goal to is to provide the best possible infrastructure to support edtech applications, the company tackles some of the toughest security challenges developers face. For instance, Clever authenticates users against a wide variety of identity providers and protocols. That means software developers can devote considerably less time and resources to writing user-authentication code for their software.

Clever also helps edtech pros with the thorny area of data transfer. “When you’re taking data from a bunch of different systems and bringing it in house, there are lots of places for things to go wrong,” Smolen says. “Because it’s what we do for a living, Clever has put a lot of thought into this area. We have the latest security protocols and we’ve vetted their implementation to ensure that data transfers are smooth—and that data is encrypted in transit and at rest.”

> At Clever, data security and privacy are at the core of our company mission. We think about it with every change we make and every new feature we introduce.
>
> **Alex Smolen**

How Clever helps

Secure Transfer

Authentication

Knowledge Sharing

As part of the edtech community, Clever likes to share its hard-earned privacy and security knowledge. You can find its award-winning privacy policy on GitHub, or peruse Clever's security whitepaper and blog to get more information on how the company protects its platform.

> When you're taking data from a bunch of different systems and bringing it in house, there are lots of places for things to go wrong.
>
> **Alex Smolen**

About Clever

Clever was founded in 2012 by educators and technologists who knew that schools, teachers, and students could all benefit from digital learning apps, but that key challenges were standing in the way of rolling them out. In five short years, more than 60,000 schools in the United States have adopted Clever. As the only platform of its kind, software developers use Clever to integrate their applications with student information systems, reducing the costs and time involved in the traditional integration process.

For more information about Clever, please contact info@clever.com

The material in this whitepaper is not legal advice and is intended to offer a broad-brush perspective. We encourage you to speak to your lawyer for advice specific to your product and team.

More resources for understanding privacy and security in education

Book

- Privacy in Context by Helen Nissenbaum

Legal Resources

- Center for Digital Education
- National Association for the State Boards of Education Webinar
- Data Quality Campaign: 2016 Legislative Summary
- National Conference for State Legislatures: 2016 Legislative Summary
- EPIC Student Privacy Project

Industry Efforts

- Future of Privacy Forum
- Student Data Privacy Pledge
- Common Sense Media
- FerpaSherpa
- Privacy Technical Assistance Center, U.S Department of Education
- iKeepSafe
- CSPA Student Data Privacy Agreement
- CDT: State Student Privacy Law Compendium
- MASS student privacy alliance - (check out Cambridge SD for a good example)

Clever

- Security at Clever
- Clever's Privacy Policy
- Clever's Terms of Service
- More whitepapers:
  > Making open standards in education work for everyone
  > The shifting landscape of student data privacy