TIP JAR

Shielding Student Data

Winter 2018
Issue 3

Today's parents face tough questions when it comes to their children's use of technology: Is my child being tracked by malicious or harmful cookies? Could my child's personal information become public? Could this technology expose my child to pornography or other harm? Parents are understandably cautious about their children using technology: Student privacy matters.

Parents entrust schools with monitoring and controlling their children's use of education technology products or services (EdTech) in the classroom. As schools increasingly use EdTech to enhance student learning and improve classroom management, they authorize third parties to store, access, and manage students' personally identifiable information. Under state and federal law, school districts must take steps to ensure that student data is protected. That is one reason why student privacy matters to school districts, too.

Know the Laws

School districts and providers of EdTech are subject to various state and federal laws designed to protect information privacy and ensure information security. Laws governing information privacy are designed to ensure that users are fully aware of how their personal information will be collected, used, retained, and disclosed. For example, the federal Protection of Pupil Rights Amendment (PPRA) regulates student surveys related to protected categories of information, including income, political and religious beliefs, and sexual behavior. School districts must provide notice to parents before administering such a survey and either obtain parent consent or allow parents to opt out for their children. Other laws governing information security are designed to prevent third parties from accessing and using personal information in unauthorized ways.

The laws governing information privacy and security of student records are extensive. While many EdTech providers are aware of the requirements of well-established federal privacy laws such as the Children's Online Privacy Protection Rule (COPPA) and the Family Educational Rights and Privacy Act of 1974 (FERPA), many have been slow to incorporate state requirements into their privacy policies and user agreements. California's Assembly Bill 1584 (AB 1584), codified as Education Code section 49073.1, requires EdTech providers to incorporate specific security and confidentiality requirements into their contracts. When EdTech providers refuse to do so, school districts must weigh the potential benefits of an EdTech product against the potential risks of violating student privacy and incurring penalties as a result.

School districts can familiarize themselves with state and federal laws applicable to EdTech through a 2016 report issued by the California Attorney General entitled *Ready for School: Recommendations for the Ed Tech Industry to Protect the Privacy of Student Data*. The California Department of Education's Data Privacy webpage and the California Attorney General's Privacy Laws webpage also provide a wealth of information.

Megan Macy
Partner and Co-Chair
Facilities & Business Practice Group
Sacramento Office
mmacy@lozanosmith.com

Penelope R. Glover
Senior Counsel and Chair
Technology & Innovation Practice Group
Walnut Creek Office
pglover@lozanosmith.com

Lozano Smith
ATTORNEYS AT LAW

Winter 2018
Issue 3

Practice Due Diligence

Ensuring adequate protections are in place to use EdTech can be daunting. With limited financial and human resources available to address EdTech and information privacy issues, school districts are burdened with the overwhelming task of assessing and negotiating agreements with each EdTech provider.

Districts may wish to leverage some of their most critical resources—teachers and librarians—by engaging them in a dialogue about the EdTech they wish to use in the classroom. Districts should consider creating a process for EdTech adoption that allows EdTech users to explain the value of the EdTech tools they want and to conduct some of the due diligence necessary to ensure these tools meet families' privacy needs. Districts can use this process to ensure legal compliance and to engage in a dialogue that will allow administrators and district staff who engage directly with students to work together to address issues ranging from compliance quandaries to union buy-in.

School districts may be able to reduce their risks by taking measures that enable them to:

- Train employees about laws designed to protect information privacy and security, especially those who use EdTech on a daily basis.
- Regularly evaluate and update privacy and security policies and practices and incorporate them into a data governance plan.
- Develop and implement procedures for vetting and evaluating EdTech.
- Obtain consents from EdTech users and provide privacy notices as appropriate.
- Bolster the EdTech evaluation process by considering external reviews by organizations like iKeepSafe, which have been approved under the Federal Trade Commission's COPPA Safe Harbor Program.
- Consult legal counsel about risks and additional protective measures.
- Communicate with the school community about the use of EdTech and the associated benefits and risks.

While such measures do not eliminate all of the risks of using EdTech in the classroom, they may mitigate them. These are complex issues and Lozano Smith's Technology & Innovation Practice Group is committed to developing practical solutions.