Managing Privacy of Electronic Student Information

A Guide for School Business Officers

Cloud-based data storage—less costly than on-site servers—and online educational tools are fueling a digital revolution in schools. For example, online applications and programs enable students to play math games and teachers to track assignments. In addition, fingerprint recognition software can speed up school lunch lines.

Such education technology has become big business. The Software and Information Industry Association estimated that the pre-K-12 education technology market was worth $8 billion in 2013. However, while schools see convenience and companies see profits, many parents are concerned about privacy and are starting to ask tough questions:

- What companies are gaining access to electronic information about my child?
- How is that information being used?
- Are companies building a file on my child?
- Could data about my child be sold to unscrupulous companies or individuals?
- Will the information create a permanent record that could later be used to harm or exploit my child?
- Do schools understand the privacy protections of websites they are using or encouraging children to use?

Federal Regulation of Online Student Information

The two main federal laws that regulate online privacy of children and students are the Children's Online Privacy Protection Act (COPPA) and the Family Educational Rights and Privacy Act (FERPA). COPPA regulates commercial online entities that either target children or knowingly collect personal information from children under 13. COPPA includes numerous obligations such as notification of parents and maintenance of a clear privacy policy. The U.S. Federal Trade Commission has imposed significant fines on commercial entities for violations of COPPA. Although schools are not subject to COPPA, they should be alert to contracts from online vendors that attempt to shift liability for COPPA to the school.

The privacy issue is of great importance to public and private K-12 schools as well as colleges that teach minors through special programs and summer camps. When schools are unable to respond to parental privacy concerns, parents are quick to organize, and contact legislators and the media. These parent groups are usually local grassroots efforts. Occasionally, they resort to legal action. For example, a Texas school district established a pilot program requiring students to carry IDs that allowed administrators to track them in the school building. The system discontinued the program after the parents of one student sued and other parents heavily criticized the system on social media.

Challenges for Schools

Safeguarding the privacy of electronic student information is challenging. Most schools do not have the resources to review every contractual agreement with the many education technology vendors used. Even when they do, they often lack expertise to analyze the implications of contractual terms. When a teacher signs students up for software and agrees to the terms and conditions on her own, school administrators many not even know the institution has entered into a legally binding agreement. For example, the developers of an application called Class Dojo estimate that one in three public school teachers have signed up their classes. The application enables teachers to reward or subtract points based on student conduct. Teachers can decide whether to display the points to the class or track student points privately. Many schools do not require teachers to obtain parental permission before using Class Dojo.

A 2013 study by researchers at Fordham University Law School showed most public school districts are behind the curve. Only 20 percent of school districts studied had policies governing the use of third-party online services. A close review of legal agreements between schools and technology companies showed that fewer than 7 percent of the contracts restricted the sale or marketing of student information by vendors. Even when contracts included such protections, many agreements allowed vendors to change the terms without notice to the school.

Federal Regulation of Online Student Information (continued)

FERPA requires educational organizations that receive federal funds to protect the privacy of student records. Exceptions exist for de-identified student information and directory information such as a student's name, home address, and email address. If a school shares student education records with an online services provider, it must notify parents and ensure the service provider is adequately protecting the records. Compliance with FERPA is important, but no educational institution has ever been fined or penalized for noncompliance. Critics contend that FERPA is poorly suited to regulating use of student information in the digital age, and many legal gray areas exist with little clear guidance from the U.S. Department of Education.

Parental Concern Is Ramping Up

Parents are often surprised that companies have access to data on their children and wonder why they were not informed by the school. Parents are not just concerned about actual data collected, such as how well their child performed on a math game. They are also concerned about metadata, such as how long a student hovers over the correct answer. The metadata may be used to determine whether a question is too difficult, but it can also be tracked back to individual students. In addition, parents are concerned that technology applications allowing users to login with their Facebook accounts can enable a company to access a student's Facebook information. Some software applications can access a student's contacts stored on a computer or smart phone.

Parents start to lose trust when educational institutions are unable to clearly and quickly articulate the benefits of educational technology and the steps taken to protect student privacy. The fate of a project called InBloom is a cautionary tale. The project was intended to help schools store data on students in a single database in a common format. Hence, schools could more easily share data with companies they selected. The project was funded by a $100 million grant from the Gates and Carnegie Foundations. While schools saw administrative convenience and the benefits of a common data format, parents saw Big Brother. They worried that a project funded by the founder of Microsoft would allow schools to sell information about their children to the highest bidder. Even though there was no evidence InBloom was actually doing what its critics charged, parents mounted grassroots campaigns through social media and fought the project state by state. The supporters of InBloom never anticipated such strong opposition. Eventually, all nine states pulled out, and InBloom folded less than two years after it started. Activists in Colorado who opposed InBloom started a group called Student Privacy Matters, which is now one of the few parental organizations advocating for student privacy at the national level.

Parents start to lose trust when educational institutions are unable to clearly and quickly articulate the benefits of educational technology and the steps taken to protect student privacy

State Legislation

Parents have also taken their protests to state legislatures. Bills protecting student data privacy were introduced in 36 states in 2014, with 16 states passing new restrictions. For example, parental protests over fingerprinting to speed up lunch lines caused Florida to pass a law prohibiting school use of biometrics. California passed the broadest and most comprehensive state legislation protecting student privacy in two separate laws, and many believe other states will follow.

California SB 1177 applies to public and private K-12 students. It prohibits online service vendors, including cloud storage services and providers of educational products, from building profiles on K-12 students except for school purposes. The vendors may not sell a student's information or target advertising on their site or any other site based on information from K-12 users. The law requires vendors to use reasonable security measures to protect student information and delete school or district controlled student information upon request. The law does not

provide penalties. However, violators could be sued under California laws governing unfair business practices that allow courts to impose fines.

A companion law, AB 1584, requires public schools that enter into contracts with online vendors of educational products or storage to ensure that the contracts contain provisions stating:

- Student records are property of the school.
- Students can retain possession and control of content they create and transfer that content to a personal account.
- The vendor cannot use any information in the student record for any purpose other than those required or specifically permitted by the contract.
- The vendor must establish procedures for a parent, legal guardian, or eligible student to review personally identifiable information in the records and correct mistakes.
- The vendor must ensure the security and confidentiality of student records.
- The vendor must establish procedures for notification of parents after unauthorized disclosure of records.
- A student's records shall not be retained or provided to a third party after completion of the contract.

Although AB 1584 only applies to public schools, it is likely that parents of students at independent schools will expect schools to exercise similar due diligence in entering contracts with vendors. The law does not specify penalties for violations.

Many experts see the California law as a roadmap for other states and Congress. The U.S. Senate introduced the Protecting Student Privacy Act in July 2014, but has not taken any action. The California law reduces challenges for schools by requiring vendors to include specific privacy provisions in contracts and prohibiting vendors from selling student information or using it for commercial purposes.

Steps for Schools

Schools outside California lack a broad statute restricting vendor access to student information. Thus, they need to take steps to ensure they are meeting parental expectations and can explain the rationale for their practices. The following are suggested steps:

- **Recognize the issue**–Many schools are still unaware of parental concerns regarding the privacy of data about their children. IT administrators, business officers, and faculty leaders need to make the issue a priority.
- **Develop a list of approved sites or vendors**–Schools need to determine which sites provide sufficient data privacy and prohibit teachers from using unapproved sites. They should explain to parents the difference between approved sites that are a regular part of the curriculum and recommended sites that may not be approved. They should also establish a clear policy on when teachers may recommend unapproved sites to students. In addition, schools should periodically update the list and make it available for parents on the school website.

Schools need to determine which sites provide sufficient data privacy and prohibit teachers from using unapproved sites.

- **Establish a vendor approval and contract review process**–The approval process needs to weigh the product's educational benefits against potential privacy concerns. The process should include a review of the vendor contract that requires terms similar to those outlined in California AB 1584. In addition, contracts should stipulate that vendors cannot sell student information or use it for marketing purposes without the express consent of the school and parents. Contracts should include clauses prohibiting unilateral modification of the contract by the vendor. In addition, the contract should state what happens to student data if a company is sold, merges, or goes out of business. More than 100 mergers and acquisitions occur every year among education technology companies. If a vendor refuses to include these contractual provisions, school administrators face a difficult decision. They can either prohibit use of the vendor or prepare a clear rationale to parents for use of its services.
- **Train teachers and administrators**–Teachers and administrators need to be sensitive to concerns about student data privacy and understand the school's policies. Many are acting independently without thinking through the implications of accepting a vendor contract. Schools need to know which sites teachers are using and conduct proper due diligence.
- **Open lines of communication with parents**–Schools need to understand parents' concerns and sensitivities. A special advisory panel that meets periodically can provide valuable input.
- **Check on insurance**–Schools should check with their liability carrier to determine whether coverage is available if the school is sued for privacy violations. Some carriers exclude this exposure entirely, and even some "cyber" policies may restrict activities covered. Also, some carriers provide helpful risk management recommendations.

The education technology field is changing rapidly with new products entering the market every month. In addition, experts predict that state legislatures will continue to pass legislation protecting student privacy. Schools need to make student privacy a top priority, establish policies, review vendor contracts, and monitor the political and technology landscape.

Acknowledgment

This publication was written by D. Frank Vinik, an attorney and risk manager who specializes in education.

United Educators

EduRisk™ provides education-specific risk management resources to colleges and schools and is a benefit of membership with United Educators (UE). As a member-owned company, UE is committed to helping educational institutions by offering stable pricing, targeted insurance coverage, extensive risk management resources, and exceptional claims handling.

To learn more, please visit www.UE.org.

UE-113211 02/15