The ABCs of Student Data Privacy for Administrators

By Andrew Bloom and Linnette Attai

The subject of student data privacy has never been more relevant, important, and stress inducing for school administrators. Although the topic has been around since the 1970s, when schools began collecting electronic information, a lot has changed since the days of analog technologies and magnetic tapes.

The size of our data universe has exploded, and most schools today are relying on cloud services to collect and store their data. The risks and responsibilities on administrators, as it relates to student data privacy, have never been greater.

This short brief covers the ABCs of student data privacy, with a goal of providing a quick overview of key privacy concepts to help you reduce risk to your school or district, and prepare you for what may lie ahead. For a deeper dive into privacy content, a list of useful resources is included on the last page.

Student Data Privacy Is Important—And It Is Your Responsibility

Student data privacy covers the use, collection, handling and governance of students' personally identifiable information (PII). This includes any and all information that can be used to identify, locate or contact an individual student—such as name, address, student ID, and login information. It also includes the student's academic, health, and disciplinary records, as well as information that can be combined to identify a particular student, like demographics and birth date.

About Andrew Bloom
As the chief privacy officer at McGraw-Hill Education since 2013, Andy has helped develop a privacy program as the business moves from a traditional publisher to a learning science company. The privacy office supports all offices and services provided by the organization around the world, including appropriate policies, procedures, and training for all applicable functions.

About Linnette Attai
Founder of compliance consulting firm PlayWell LLC, Linnette is an expert in privacy, safety and marketing regulation and self-regulation in the education and entertainment sectors. She has over 25 years of experience creating industry and school compliance programs, and also currently serves as project director for the CoSN Privacy Initiative and Trusted Learning Environment program.

Simply put, student data privacy is important because there are legal and ethical limitations on the collection, use, sharing, and handling of student PII. Federal and state laws regulate the privacy of student PII—and while enforcement has been historically lax, the legal landscape is changing.

Meanwhile, data collection and the use of student information inside and outside our schools is rising all the time. Plus, administrators are outsourcing data services and bringing more technology into the classroom, resulting in a greater number of contracts with information technology (IT) service and solution providers—and more for schools to manage.

This evolution should serve as a wake-up call for all administrators. The bottom line is that schools are legally and ethically obligated to keep student PII private—regardless of where and how the student data is created, used, or stored.

Fundamentals of Current Federal Privacy Laws

Regulation around student data privacy is evolving. While the majority of legislative activity is happening at the state level, there are a few longstanding federal laws. Administrators should at least become familiar with the following three:

1. Family Educational Rights and Privacy Act (FERPA)

FERPA was signed into law in 1974 to allow parents and students age 18 and older (referred to as eligible students) access to their school records. Overseen by the US Department of Education (DOE), the law applies to educational institutions that receive federal funding, and grants four specific rights to the parent and eligible student:

- The right to see the student's education record.
- The right to seek an amendment to those records if they are misleading, inaccurate, or in violation of the student's privacy rights, and, in certain cases, append a statement to the record.
- The right to consent to disclosure of personally identifiable information in the education record.
- The right to file a complaint with the Family Compliance Policy Office in Washington, DC.

Failure to comply with FERPA exposes school districts to a loss of federal funding, though the DOE has not yet imposed this penalty on any institutions.

2. Protection of Pupil Rights Amendment (PPRA)

PPRA was passed into law in 1978 and applies to programs and activities funded by the DOE. It allows parents to review marketing surveys and also to grant or deny permission for their minor child to participate in surveys, analyses, and evaluations that require the student to reveal information about themselves or their family that deal with sensitive subject matter, such as:

- Religious practices, beliefs, or affiliations
- Political affiliations or beliefs
- Mental health problems
- Sex behavior or attitudes
- Illegal or self-incriminating behavior
- Critical appraisals from others close to the student or family
- Legally recognized privileged relationships (i.e. doctors, ministers, lawyers)
- Income (other than as required by law to determine program eligibility)

As with FERPA, the rights given to the parent transfer to the student once the student reaches the age of 18.

3. Children's Online Privacy Protection Act (COPPA)

COPPA was enacted in 1998 to protect the privacy of children under the age of 13 while online. Enforced by the Federal Trade Commission (FTC), the law requires operators of websites and online services that target or knowingly collect PII from children under 13 to obtain verifiable parental consent before doing so and keep the information secure.

Unlike FERPA and PPRA, COPPA applies directly to technology operators, although in certain situations, operators may rely on the schools to obtain the required verifiable parental consent.

Legislation at the State Level is Booming

The exponential growth of technology used in schools has resulted in a recent flurry of student data privacy legislation at the state level. According to the Data Quality Campaign, from 2013 to 2016, 49 states introduced over 400 bills related to student data privacy. To date, 73 of those bills have been signed into law across 36 states—and the number is growing.

While policy strategies vary from state to state, these new laws have common threads. For example, they tend to focus on the following themes:

- Establishing additional safeguards for the collection, use, and disclosure of PII.
- Governing the permissible activities of online service providers.
- Prohibiting service providers and districts from selling or profiting from PII.
- Expanding existing regulatory definitions of personally identifiable information.

As a school administrator, it is important to keep an eye out for new and pending student data privacy legislation at the state level. If recent events are any indication, if you have not been affected yet by new data privacy regulations, you may be soon.

Know Your Data—and Your Data Contracts

An important first step in developing effective student data privacy policies and procedures for your school is understanding all of the student data you have. This may sound obvious, but it's something many districts fail to consider before jumping into creating policy.

The best way to discover the data you have is by doing a data inventory and mapping all the automated and manual processes that collect or use student information. Once you understand what data is being collected and how it is used, you can properly secure it.

As an administrator, you will realize the benefits of the data inventory and mapping quickly. First, you will be able to create thorough and transparent privacy information to be shared with parents and students. Second, you will be able to communicate more effectively with employees and vendors about data-related issues, practices, and requirements. Finally, you will be able to better identify any areas where you might be unnecessarily collecting data, or where you might not be protecting data as well as you could be.

Just as important as knowing the data you have is ensuring that contracts with third parties reflect privacy requirements. The school is ultimately responsible for how vendors use the data, so even though you may have counsel to review your school's legal contracts, it is important that you know what to look for—and what to look out for—in data service agreements.

Before contracting with any IT vendor, make sure they understand the student data privacy laws in your state, as well as your district requirements. Contracts with vendors should be clear about how their system will interact with your data—including where and how it will collect, store, and protect the information and, if appropriate, how their system will securely destroy it.

In Conclusion

Because student data privacy is a critical and growing issue nationwide, it is imperative that all schools have a clear understanding of the issues at hand as well as a clearly outlined policy that covers data privacy within their school or district, as well as for those who work with them (contractors, IT vendors, etc.). Local and federal laws will continue to change and evolve over time, and a foundational policy and plan will help keep up with the rapid changes and growing demands of data privacy. For further reading and information, see the links and resources below.

Resources

FERPA | SHERPA (ferpasherpa.org) provides service providers, parents, school officials, and policymakers with easy access to materials and resources to help guide responsible uses of student's data.

US Department of Education Privacy Technical Assistance Center (PTAC) (ptac.ed.gov) is a resource for education stakeholders to learn about data privacy, confidentiality, and security practices related to student-level longitudinal data systems and other uses of student data.

Protecting Student Privacy While Using Online Educational Services: Model Terms of Service (ptac.ed.gov/sites/default/files/TOS_Guidance_Mar2016.pdf) the PTAC, working with the Department of Education's Family Policy Compliance Office, has developed guidance for evaluating vendor Terms of Service Agreements. This document is intended to assist users in evaluating potential agreements and understanding commonly used terminology.

CoSN Privacy Toolkit for School Leaders (cosn.org/focus-area/leadership-vision/protecting-privacy) provides school officials with 10 essential skills areas, outlining the responsibilities and knowledge needed to be an educational technology leader.

CoSN Trusted Learning Environment Program (trustedlearning.org) provides school systems with measurable steps to implement practices to help ensure the privacy of student data.

Data Quality Campaign (dataqualitycampaign.org/action-issues) provides information on state laws annually, as well as other useful privacy review tools and resources.

What is student data? (dataqualitycampaign.org/wp-content/uploads/2016/02/What-Is-Student-Data.pdf) DQC guidance on what constitutes student data.

ConnectSafely Educator's Guide to Social Media (connectsafely.org/eduguide) explains how educators can use social media in the classroom without risking their professional reputation.

ConnectSafely, FPF, PTA Parent's Guide to Student Data Privacy (ferpasherpa.org/pdf/parents_guide.pdf) assists parents in understanding the laws that protect student data and helps parents understand their student's rights under the law.

PF16 M 08483