iKeepSafe
PEACE OF MIND FOR FAMILIES ONLINE™

STUDENT DATA PRIVACY AND SECURITY: A ROADMAP FOR SCHOOL SYSTEMS[1]

Managing student data privacy and security is an active process, requiring ongoing attention and vigilance. This roadmap is intended as a guide for school districts to better understand the keys to implementing comprehensive compliance programs, which serve as frameworks for ensuring safe and healthy use of technology in education settings.

I. STUDENT PRIVACY: POLICIES AND PROCEDURES FOR SCHOOL SYSTEMS

A. Privacy Program

A comprehensive and systematic approach to privacy will help schools avert privacy missteps and the resulting harm, including costly legal actions. With the appropriate policies, training, oversight, and auditing, schools can dramatically limit their exposure to very damaging privacy mistakes that can hurt students, the school's reputation and the entire education community.

[1]The information in this memorandum was developed with input from leading experts in privacy including Professor Daniel Solove, the John Marshall Harlan Research Professor of Law at the George Washington University Law School (http://danielsolove.com), and industry compliance expert Linnette Attai, President and Founder of PlayWell, LLC (http://playwell-llc.com).

A good privacy program will do the following:

- Identify and minimize risks of a privacy mishap
- Document an incident response plan
- Keep policies up-to-date in light of changing technologies and laws
- Train employees about how to deal with privacy issues
- Educate students and parents about privacy issues

Implementing a formal and robust privacy program will help to ensure the privacy of everyone in the school community is protected—students, parents, educators, employees, applicants, and others.

B. Privacy Assessment

A privacy assessment, conducted by an independent third party, can provide necessary information and direction for school systems seeking to enhance their data privacy and security policies and practices.

A privacy assessment will identify:

- Risks, gaps in policy, and areas where policies are misunderstood or are not being followed
- Policies that need to be updated in light of new laws and technologies
- Types of data collected by various departments, how they use it, who has access to it, and how securely it is being maintained
- Student data collected through technology used by the school, in and outside of the classroom

C. Establish an e-Safety Committee and a Privacy Point Person

An e-safety committee should be established to review privacy audits, monitor ongoing compliance, recommend policy and practice changes and manage privacy-related communications. It should be comprised of multiple stakeholders (e.g., principals, network administrators, counselors, school resource officers, media instructors, health and technology specialists, etc.). The committee should have a dedicated privacy point person at both the school and district level who understands how the school is addressing all privacy issues, and knows where to go for answers to questions from the school community.

D. Policies and Procedures

A school system's policies should articulate a set of privacy practices that a school will follow, such as providing notice to people (students, parents, employees, etc.) regarding the data collected about them. The policies should also establish rules for key practices, such as maintaining confidentiality, security and integrity of the data it holds, identifying circumstances when the school will disclose data without consent, and how the school will communicate future policy changes. The policies should be drafted in language that is clear and easily understood by all of the intended audiences. In addition, a school should train and certify all employees on the policies.

II. PRIVACY RISKS AND ISSUES FOR SCHOOL SYSTEMS

A. Confidentiality and People in Distress

Have a policy in place and train employees to address the issues around confidentiality involving people in distress. These situations can be quite challenging, and failure to share information appropriately can lead to tragic consequences.

B. FERPA Compliance

The Family Educational Rights and Privacy Act (FERPA) provides a set of rules for how schools can use and disclose education records. It provides parents (and eligible students) with a set of rights, and it requires that schools provide notice to parents about those rights. FERPA issues include:

- Annual FERPA notice to parents
- Directory information
- Sharing of data
- Emergency situations
- Responding to law enforcement requests for data
- Responding to subpoenas and court orders
- Providing parents and eligible students with access to data
- Disciplinary records
- Technology assessments
- Vendor contracts and record-keeping
- Record-keeping of data collected and disclosures

C. COPPA Compliance

The Children's Online Privacy Protection Act (COPPA) mandates that operators of websites or online services directed to children obtain verifiable parental consent prior to the collection, use or disclosure of certain personal information from children under the age of thirteen. It allows the option for schools to act in lieu of parents in providing consent in certain, but not all, circumstances. COPPA issues to consider:

- Technology assessments
- Privacy policy review
- Contracts and record-keeping
- School consent determinations and limitations
- Parental consent notices and requests

D. CIPA Compliance

The Child Internet Protection Act (CIPA) requires that schools employ software or other technology to block access to inappropriate materials. It also requires that schools ensure the safety and security of minors who use certain electronic communication methods, and prevents unauthorized disclosure, use and dissemination of personal information regarding minors. Some of the issues schools should consider related to CIPA include:

- Assessment of technology filters
- Safety education curriculum and planning
- Public notice and meetings
- Acceptable use policies
- Internet monitoring policies
- Disciplinary policies and procedures

E. PPRA Compliance

The Protection of Pupil Rights Act (PPRA) is designed to protect the privacy of students in surveys, medical exams and marketing programs. PPRA applies to all schools (except postsecondary schools) that receive funding from the U.S. Department of Education or participate in surveys funded in any amount by the Department of Education. Depending on the information collected, the PPRA mandates that schools comply with opt-in or opt-out requirements.

F. Online Communication and Social Media

School policies addressing civil discourse on and off campus should provide employees, students and parents with clear guidance about how the school will respond to harmful or distressing speech within the limits of the First Amendment. Articulate a balance between robust expression of ideas and restrictions on invading others' privacy, defaming others, creating a hostile environment, or otherwise harming individuals through speech.

G. Incident Response

1. Data Security Breach Response Plan

Data breaches happen with surprising frequency. In addition to continuously assessing and improving security protocols, a quick and effective response can play an enormous role in minimizing the damage.

2. Behavioral Incidents Response Plan

Responding to digital incidents such as cyberbullying, online gossip, and sexting requires clear policies, training, and incident response plans to ensure they are handled appropriately and with consideration of the privacy implications.

H. Sharing Personal Data with Third Parties

1. Selecting Third Party Vendors

Prior to selecting third party vendors that will receive student data (such as cloud service providers), ensure that the third parties understand the school's legal obligations around student data privacy and security, and have appropriate compliance policies and practices in place. Review details about how the vendors use, store, and protect the data, as well as who might have access to the data and why.

2. Contracting with Third Party Vendors

When contracting with a third party service provider, be sure that the contract clearly identifies what data will be collected, ensures that the data is protected and its uses are appropriately limited, and that effective oversight and accountability mechanisms around privacy, security and the contractual terms are in place.

I. Use of Technology

1. Devices and Software

Design policies and training to ensure that school administrators and educators understand the implications of using various products that may collect student data. At one school district, school personnel used software to capture photographs taken by webcams from computers lent to students. This led to a lawsuit, congressional hearings, and an FBI investigation. Just because various technological tools and services are sold on the open market does not mean they are legal to use in schools or that their use is advisable.

2. Websites and Online Services

Educators often bring technology into the classroom, requiring that students use a particular website, app or other online service. Prior to using these services, assess the privacy, security and terms of use policies and examine the legal implications of using these products. Train educators to understand that certain uses of these tools and services could violate the law or create significant risks of a data breach or privacy incident.

J. School Websites

Ensure school websites include a privacy policy that reflects actual practices and complies with the laws that regulate Internet privacy, including the Children's Online Privacy Protection Act (COPPA) and the California Online Privacy Protection Act (calOPPA).

K. Searches and Surveillance

1. Searches of Electronic Devices

As more electronic devices are being used at school, school systems must have policies in place for searching and seizing those devices in ways that do not run afoul of the Fourth Amendment or state and federal electronic surveillance and computer access laws.

2. Surveillance

Schools have a number of opportunities to conduct video and audio surveillance. A school system's policies should clearly identify if, when, where and how to engage in video or audio surveillance, as there are strict and complicated federal and state laws with which to comply.

L. Data Security

1. Administrative, Physical, and Technical Safeguards

Security protocols and practices should be assessed and upgraded regularly. Appropriate administrative, physical, and technical safeguards will help to protect data and networks from being compromised.

2. Data Disposal

Proper data deletion and disposal, including purging electronic data, shredding physical documents and destroying old electronic equipment where data had once been stored, are important components of a data security practice.

3. Removal of Data from School Grounds

Lost or stolen laptops and USB drives are a frequent cause of data security breaches. School policies surrounding the acceptability of removing equipment from campus or accessing data remotely can help reduce this risk.

III. Education and Training

A. Who Should be Educated?

Students. Educating students about protecting their online privacy and becoming savvy digital citizens is essential to helping them understand the consequences of their activity online. It will help them protect themselves and learn to manage key parts of their lives in the digital age.

Parents. Educating parents about technology being used in the classroom and their rights around student data privacy and record access is also of vital importance. Parents need to know the challenges and opportunities that technology provides their children. And they need to know what to do to protect themselves and their children.

Educators. Educators will benefit greatly by being more informed about data privacy and security regulations and norms, the pitfalls that can happen when technology is not assessed properly before being introduced into the classroom, and perils that they and their students may face around technology incidents. Educators also need to be trained about how to deal with incidents such as cyberbullying, harassment and sexting, which can invade the classroom environment through technology.

Administrators (including network administrators). Administrators will benefit by improving their skills and competencies around student privacy. Administrators need to know the requirements and boundaries of regulations, what policies and procedures should be in place before an incident occurs and how to ensure the community can have confidence in the services and technologies utilized by their schools.

B. What Should We Teach Educators and Administrators?

Since protecting privacy and data security depends so heavily upon employee compliance with policies, most companies that collect and maintain personal data provide annual privacy and data security training. Policies are meaningless if people don't know what they need to do to comply with them, why it is important that they follow the policies, and when they should ask questions before acting. As with other industries, schools would benefit greatly by training their personnel. Training on most topics should be conducted annually.

Below is an outline of a recommended training curriculum for school personnel:

Basic Privacy Awareness

1. What is privacy?
   - » Generally recognized privacy principles
2. Why does privacy matter?
   - » The importance of protecting privacy

Privacy Rights and Responsibilities

1. The Federal Educational Rights and Privacy ACT (FERPA)
   - The key requirements of FERPA that apply to all teachers, employees, and school officials that will have access to student data

2. Confidentiality and people in distress
   - When and how to share data about people in distress

Data Security

1. Data security awareness
   - Protecting data so that it doesn't fall into the wrong hands
   - How data security depends upon everyone at the school

2. Phishing and online threats
   - Avoiding malware, phishing, and other online threats

3. Data security best practices
   - Data security best practices. Treatment of portable devices, passwords, data disposal, physical access, etc.

Online Communication and Social Media

1. Online gossip and self-exposure
   - School policies around monitoring and reporting inappropriate content posted on social media
   - Tools and tips for helping students develop a positive online profile and reputation
   - The harms that may befall students from online gossip and self-exposure
   - Dealing with incidents involving online gossip and rumor
   - How educators can use social media responsibly

2. Cyberbullying
   - Providing protection and ongoing support to victims of cyberbullying
   - Responding to cyberbullying incidents at the school

3. Sexting
   - The legal, social and emotional dangers of sexting
   - Dealing with sexting incidents

Electronic Searches, Surveillance, and Access

1. Searches and surveillance
   - » The legality of various kinds of searches and surveillance by school personnel

2. Unauthorized access to electronic devices and accounts
   - » Privacy violations and legal repercussions
   - » Policies around confiscation of electronic devices

IV. CONCLUSION

iKeepSafe recognizes that schools and parents want to ensure that the education community is equipped to take the lead on protecting student data, and ensuring that technology used in the education setting is compliant with existing rules and regulation around privacy and security. Developing robust and comprehensive data privacy and security policies and practices is the first step in the process, and it is our hope that this roadmap will help set the stage for school systems to better protect their community stakeholders.

About iKeepSafe:

iKeepSafe is 501(c)(3) nonprofit international alliance of more than 100 policy leaders, educators, law enforcement members, technology experts, public health experts and advocates. iKeepSafe provides credible and comprehensive privacy information, services and curriculum at no cost to educators, industry, parents and policymakers to help empower and inform those responsible for bringing technology into the classroom environment.