iKeepSafe recognizes that schools and parents want to ensure that technology and services used in the education setting protect student data and are compliant with existing rules and regulation around privacy and security. iKeepSafe provides credible and comprehensive privacy information, services and curriculum at no cost to educators, industry and policymakers to help empower and inform those responsible for bringing technology into the classroom environment.

I. STUDENT PRIVACY: POLICIES AND PROCEDURES FOR COUNTIES, DISTRICTS AND SCHOOLS

A. Privacy Program

To protect privacy adequately, all schools should develop a comprehensive privacy program. 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

1The 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/about-us).
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. A comprehensive and systematic approach to privacy will help schools avert privacy debacles 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.

B. Privacy Assessment

Schools should begin by conducting a privacy assessment, preferably by an independent third-party skilled in this work. The privacy assessment is a way to identify risks, gaps in policy, and areas where policies are misunderstood or are not being followed. The assessment is also a way to identify policies that need to be updated in light of new laws and technologies. The assessment should include an accounting of what kinds of data various departments are collecting, how they are using it, who has access to it, and how securely it is being maintained. The same information should be gathered for student data being collected through technology used by the school, in and outside of the classroom. The assessment should not just focus on policies but also on practices. Additionally, the assessment should seek to identify areas where personnel are confused or have questions. The assessment should be used as the launchpad for improving and enhancing data privacy and security policies and practices.

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

It is recommended that all schools and districts establish an e-safety committee comprised of multiple stakeholders (e.g., principals, network administrators, counselors, school resource officers, media instructors, health and technology specialists, etc.). The e-safety committee needs a dedicated privacy point person at the school and district level who has an understanding of how the school is addressing all privacy issues, and knows where to go for answers to questions.

D. Policies and Procedures

A school’s policies should articulate a set of privacy practices that the school will follow, such as providing notice to people (students, parents, employees, etc.) regarding the data collected about them. The school’s policy should also establish rules for key practices such as maintaining confidentiality and security of the data it holds, identifying circumstances when the school will disclose data without consent, and how the school will communicate future policy changes. This policy 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 data confidentiality policies.
II. SPECIFIC PRIVACY RISKS AND ISSUES

A. Confidentiality and People in Distress

A school should have a policy and training to address the issue of confidentiality and people in distress. These situations can be quite challenging, and failure to share information appropriately can lead to tragic consequences.

B. FERPA Compliance

A school should have policies, procedures, and training in place in order to comply with the Family Educational Rights and Privacy Act (FERPA). 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. Some of the FERPA issues schools should focus on 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
» Disciplinary records
» Parental access and communications
» Technology assessments
» Vendor contracts and record-keeping
» Record keeping of data collected and disclosures

C. COPPA Compliance

A school should have policies, procedures and training in place in order to comply with the Children’s Online Privacy Protection Act (COPPA). 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
D. CIPA Compliance

A school should have policies, procedures and training in place to ensure compliance with the Child Internet Protection Act (CIPA). 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 it 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

A school should have policies, procedures and training in place to ensure compliance with the Protection of Pupil Rights Act (PPRA). 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 provide opt-in or opt-out requirements.

F. Online Communication and Social Media

A school should have a policy in place to address civil discourse on and off campus. A school 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 to the U.S. Constitution. A school must 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. This balance must be struck for students as well as employees.

G. Incident Response

1. Data Security Breach Response Plan

A school should have a data security breach response plan in place. Breaches happen with surprising
frequency, and a quick and effective response can play an enormous role in minimizing the damage.

2. Dealing with Incidents

A school should implement policies and training for employees about how to deal with incidents such as cyberbullying, online gossip, and sexting, and the privacy implications and concerns that may arise when investigating such situations.

H. Sharing Personal Data with Third Parties

1. Selecting Third Party Vendors

A school should have a methodical approach to selecting third party service providers that will receive student data (such as cloud service providers). Prior to engaging in business with a third party, an educational institution should conduct due diligence on the entity and make sure that the provider understands the legal requirements around student data privacy and security, and has appropriate compliance policies and practices. The educational institution should review details about how the service provider uses, stores, and protects 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, an educational institution should 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. School Administrators Use of Tools and Services Involving Student Data

Schools should have policies and procedures to ensure that school administrators and educators understand the implications of using various tools and services involving student data. At one school district, school personnel used software to capture photographs taken by webcams from computers lent to students. This practice 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 in certain contexts.

2. Educator Use of Technology and Online Services

Educators often bring technology into the classroom, requiring that students use a particular website, app or other online service. Schools should make sure that the privacy, security and terms of use policies for each product are assessed and that the legal implications of using these tools and services are examined in
advance of introducing the technology in the classroom. Schools should 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

A school should have privacy policies on its websites that reflect actual practices, and be mindful of 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

A school should have policies in place for searching and seizing electronic devices in ways that do not run afoul of the Fourth Amendment to the U.S. Constitution or state and federal electronic surveillance and computer access laws.

2. Surveillance

A school should have policies for 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

Schools should have in place the appropriate administrative, physical, and technical safeguards to protect data and networks from being compromised.

2. Data Disposal

A school should have policies for proper data deletion and disposal, including shredding physical documents and destroying old electronic equipment where data had once been stored.

3. Removal of Data from School Grounds

Schools should have policies regarding the acceptability of removing data from campus, as lost or stolen laptops and USB drives are a frequent cause of data security breaches.
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 help students understand the consequences of their activity online. Educating students will help them protect themselves and learn to manage key parts of their lives in the digital age.

Parents. Educating parents on 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 dangers, challenges and opportunities that technology provides their children. And they need to know what to do to protect themselves and their children.

Educators. Educators need to be educated too. Educators will benefit greatly by being more informed of 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?

Most companies that collect and maintain personal data about their employees provide annual privacy and data security training. Because protecting privacy and data security depends so heavily upon employee compliance with policies, training is essential. Policies are meaningless words on a page 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 personal 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 and other online threats

3. Data security best practices
   - Best practices for data security (treatment of portable devices, passwords, data disposal, physical access, etc.)

Online Communication and Social Media

1. Online gossip and self-exposure
   - Popular social media websites children are using and school policies around monitoring and reporting inappropriate content
   - Tools and tips for developing 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
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

Managing student data privacy and security is an active process, requiring ongoing attention and vigilance. iKeepSafe remains available to help educators, parents and policymakers better understand the keys to implementing comprehensive programs to continue ensuring safe and healthy use of technology in education settings.