Protecting Privacy in Connected Learning Toolkit

Moving From Compliance to Trust

VERSION 3, JUNE 2017

CoSN
LEADING EDUCATION INNOVATION

Protecting Privacy
in Connected Learning
A CoSN Leadership Initiative

Protecting Privacy in Connected Learning Toolkit

Moving From Compliance to Trust

VERSION 3, JUNE 2017

Protecting Privacy
in Connected Learning
A CoSN Leadership Initiative

Sponsored by

filewave
Multi-Platform Endpoint Management

hp

Mc Graw Hill Education

Microsoft

Disclaimer: CoSN is a professional association comprised of school system technology leaders, not lawyers. While we aim to provide valuable tools to help you navigate these issues, you should not rely solely on these tools for legal advice. In all circumstances, please seek appropriate legal or other professional advice regarding specific facts and circumstances pertaining to your school system. This document does not cover all privacy law or policy. You should always consult your legal counsel to understand how federal, state, and local laws and policies may apply to your school system.

About CoSN

CoSN (the Consortium for School Networking) is the premier professional association for School System technology leaders. For nearly 25 years, CoSN has provided leaders with the management, community building and advocacy tools they need to succeed. Today, CoSN represents over 13 million students in school districts nationwide, and continues to grow as a powerful and influential voice in K-12 education. CoSN empowers education leaders to leverage technology to create and grow engaging learning environments.

About This Resource

The CoSN Protecting Privacy in Connected Learning Toolkit supports School Systems in understanding the issues that arise when navigating student data privacy responsibilities, including the selection and use of an online service provider.

The original version of this document focused on key requirements of the Family Educational Rights and Privacy Act (FERPA) and the Children's Online Privacy Protection Act (COPPA). This most recent version, released in June 2017, refreshes almost every section of the Toolkit, and includes expanded material on Directory Information and the Protection of Pupil Rights Amendment. It also includes new sections on how key federal data privacy laws operate together, as well as the National Student Lunch Act.

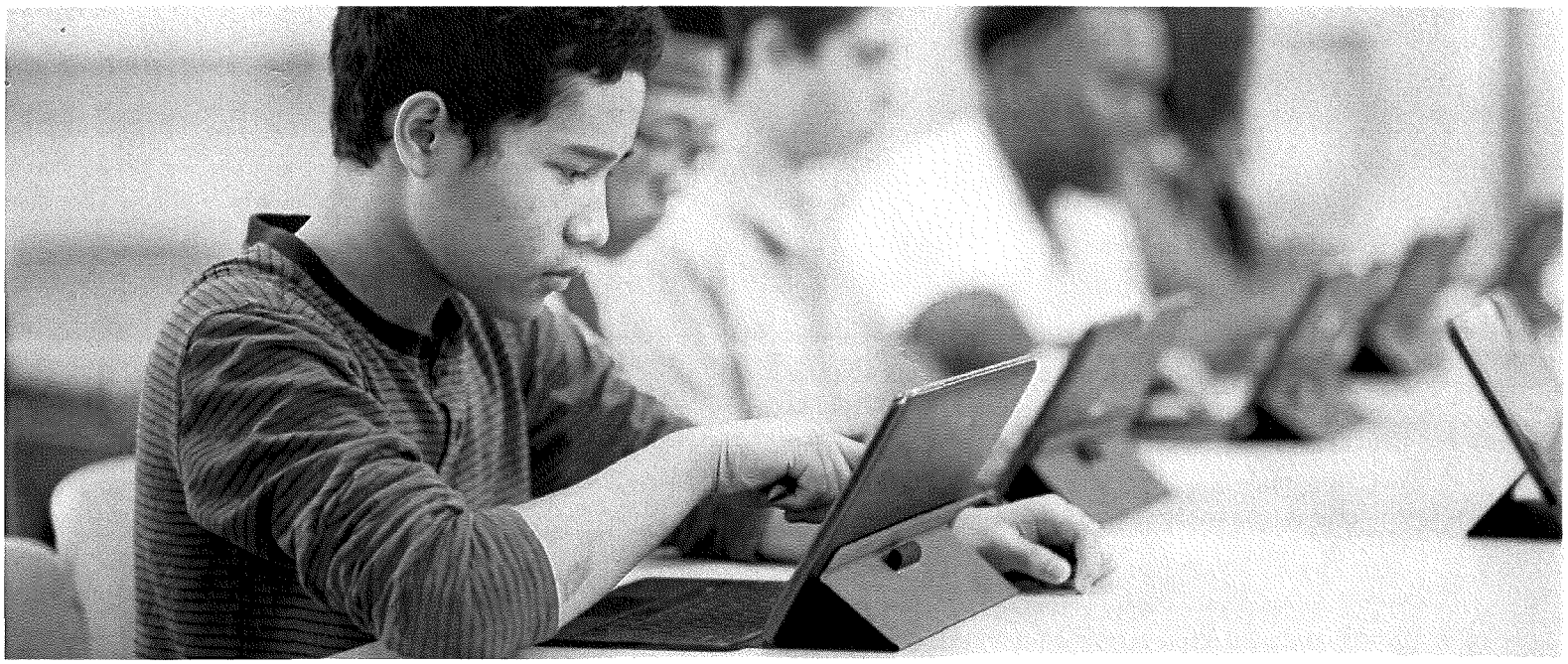
The Toolkit offers detailed definitions of terms such as Education Record and School Official, suggested Contract Terms and Security Questions for Service Providers, and explanations of issues related to metadata and data de-identification. The Toolkit also includes guidance related to the use of Click-Wrap Agreements, common to so many popular, free online tools and services. A set of helpful links to privacy-related resources is also included.

Because it is important to consider privacy and security decisions in the context of **compliance, potential harm and the need for transparency**, the Toolkit includes a decision tree. FERPA and COPPA compliance issues are addressed, as are suggested practices that reach beyond compliance.

It should be noted that this document only covers some of the obligations that School Systems have in protecting the privacy and security of student data, and this Toolkit should not be construed as legal advice. In addition, School Systems may be subject to other federal and state privacy laws that are not covered here, and every circumstance requires a case-by-case analysis under the law. Please check with your School System's legal counsel to understand how federal, state, and local laws may apply to your School System.

Disclaimer: CoSN is a professional association comprised of school system technology leaders, not lawyers. While we aim to provide valuable tools to help you navigate these issues, you should not rely solely on these tools for legal advice. In all circumstances, please seek appropriate legal or other professional advice regarding specific facts and circumstances pertaining to your school system. This document does not cover all privacy law or policy. You should always consult your legal counsel to understand how federal, state, and local laws and policies may apply to your school system.

Table of Contents



Introduction

Today's classroom sits in stark contrast to those of just a few years ago. Educators, students and parents are now benefitting from exciting opportunities, available as a result of new instructional technologies, including cloud-based technology services, connected devices and mobile applications. These technologies enable rich, data-powered classroom experiences, drive administrative efficiencies and provide students with the "anytime, anywhere" learning environment that education technologists and others have envisioned for many years.

However, with these possibilities come challenges, and as technology comes into schools, so does the need to manage the risks associated with these technologies. Managing risk is not a new challenge for schools. Schools are continuously assessing risk and identifying and implementing an appropriate response, whether it be mandatory use of goggles in the chemistry class, safety gear and appropriate physical fitness for the football field, monitoring activity on the school bus, or now, assessment and contractual controls around vendor management of data.

With cloud services and other technologies, schools must manage legal compliance and also find a balanced approach between other types of risk, and rewards, including instructional goals. The work requires that each School System choose the measures appropriate to their ecosystem (e.g., governance policies, contract clauses, security requirements, etc.) to help mitigate the risk while still allowing for innovation.

There are *three areas districts must address*:

- **Compliance** (with federal and state laws, board policy and contracts);
- **Harm** (to the student, or the school, for example through a breach of sensitive data); and
- **Perception** (by the school's stakeholders: parents, students, teachers and school board or legislative representatives)

In order to **move from compliance to trust**, schools should continue to **raise the bar** on existing compliance practices with **concrete policies and practices** to provide **appropriate protections** for student data. They must also **communicate** those practices to parents in order to ease their concerns about student data privacy and **earn the trust** of community stakeholders.

It's no easy task. The policies and practices needed to comply with existing federal and state privacy regulation are complex, and the climate is shifting, with new state privacy laws being introduced at record pace. In addition, compliance with regulation is generally considered to be the floor, not the ceiling. To truly protect the privacy and security of student data, School Systems need to understand what the laws require, how to implement those laws effectively across multiple technologies, and how to align with community expectations regarding data privacy and security in order to best leverage the power of information and technology to support student success.

Section 1: Understanding Your Data Privacy Responsibilities

Getting Started

What does a school privacy management program look like, who needs to be involved and what are the fundamental practices that schools should have in place to effectively manage data privacy and security responsibilities in a way that protects students, ensures compliance, and engenders trust in the community?

According to the US Department of Education's (ED's) Privacy Technical Assistance Center (PTAC), an effective student privacy program improves the efficiency of district decision-making and operations regarding data collection, disclosure, and use of student data. In addition, a student privacy program:

- Helps districts meet legal and ethical requirements for protecting personally identifiable information in student Education Records.
- Protects students from harm (e.g., identity theft, discrimination, predatory activity); and protects the district from harm (e.g., loss of public confidence, administrative burden of investigating a breach, alienating parents, financial loss).
- Improves communication and transparency with parents and students about data practices, and reassures parents and students about the security of their personal information.

Whether you're just getting started with your approach to protecting the privacy of students, or are looking to improve your practices, a fundamental part of the process should be establishing your own frameworks of behavior around management of student data. Even if something is legally allowed, that does not mean that it will be the right fit for your School System. Three useful starting points for frameworks are Ten Steps Every District Should Take Today, PTAC's Checklist for Developing School District Privacy Programs and the National Forum on Education Statistics Guide to Education Data Privacy.

Here are some key steps you'll need to manage:

1. Get leadership to acknowledge the need for a program.
2. Designate individual responsible for policies relating to data use and privacy.
3. Bring the right people to the table
4. Determine which policies and procedures are already in place.
5. Adopt any additional necessary policies and procedures for the use of student data throughout the data life cycle, including consequences for non-compliance.
6. Train data users on relevant policies and procedures.
7. Think about how best to be transparent to parents and students about privacy.
8. Develop a monitoring plan to ensure policies and procedures are being followed.

To begin the conversation with leadership, we encourage you to review the Student Data Principles. The Principles were created by a coalition of national stakeholders led by CoSN and Data Quality Campaign, who set out to determine a set of fundamental beliefs for using and protecting student data to guide the work of the education community.

With the right players at the governance table, this Toolkit serves as a resource to aid school districts in understanding their compliance requirements, identify and evaluate potential harms and plan effective, transparent communication.

School System: an educational agency, including a school, district or local education agency

Provider: a technology company, or "operator," that delivers Internet-enabled products and services, such as websites, apps and data management platforms to a School System

Privacy: practices around the collection, use, handling, disclosure and deletion of personally identifiable information.

Security: protections preventing unauthorized access to the data and preserving the confidentiality, integrity and availability of the information.

Privacy and **security** are related disciplines, but they are not interchangeable.

Statutory Definitions: Federal student data privacy laws define similar terms in different ways, and it's important to understand the distinctions. Please also note that state laws include different definitions of similar terms. Be sure to familiarize yourself with the definitions presented here and compare them with definitions that may be included in your state's student data privacy legislation. By considering the entire ecosystem of legal definitions, you'll be better positioned to properly assess your data privacy practices.

STATUTORY DEFINITIONS

FERPA DEFINITIONS	COPPA DEFINITIONS
▸ **Personally Identifiable Information (PII):** Includes, but is not limited to: the name of a student or family members, the address of a student or family members, a personal identifier, such as the student's social security number, student number, or biometric record, other direct or indirect identifier that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty, and information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the Education Record relates.	▸ **Personal Information (PI):** Individually identifiable information collected online from a child under the age of 13, including: First and last name; address or other geolocation information that identifies a street name and city or town; email address or other online contact information that allows direct contact with a person online, including a screen or user name that functions in that same manner, telephone number, Social Security number; a persistent identifier that can be used to recognize a user over time and across different Web sites or online services, photograph, video, or audio file that contains a child's image or voice, or information about the child or the child's parents or legal guardians that the operator collects online from the child and combines with one or more of the above identifiers.
▸ **Education Records:** Materials that are "maintained by an educational agency or institution or by a party acting for the agency or institution," and that contain information directly related to a student. For more information about Education Records, including details of what is not considered an Education Record, see below.	

Disclaimer: CoSN is a professional association comprised of school system technology leaders, not lawyers. While we aim to provide valuable tools to help you navigate these issues, you should not rely solely on these tools for legal advice. In all circumstances, please seek appropriate legal or other professional advice regarding specific facts and circumstances pertaining to your school system. This document does not cover all privacy law or policy. You should always consult your legal counsel to understand how federal, state, and local laws and policies may apply to your school system.

FERPA DEFINITIONS	COPPA DEFINITIONS
▶ **Directory Information**: Information in the Education Record that is not considered to be harmful or an invasion of privacy if released. **Each School System must define what it considers to be Directory Information**, which may include a student name, address, telephone number, email address, photograph, date/place of birth, major, grade level, enrollment status, date of attendance, degrees, honors/awards, most recent educational institution attended, and participation in officially recognized sports and other activities, and weight and height of members of athletic teams. Directory Information may not include a social security number or student ID that may be used to gain access to Education Records without additional information. For more information about Directory Information, see **Directory Information FERPA Exception.**	
▶ **De-Identified Data**: All personally identifiable information has been removed and a reasonable determination has been made that a student is not personally identifiable, whether through single or multiple releases of information, and taking into account other reasonably available information. For more on De-Identified Data, and a discussion of aggregated data, see **Understanding Metadata and De-identification**.	

Education Records

Just what is or is not an Education Record is not always clear-cut. Be sure to ***assess whether or not the records or information being collected, generated, stored or processed by a Provider qualify as an Education Record with your School System's legal counsel*** before proceeding. If they are, you will need to ensure that the handling of those records is done in alignment with FERPA requirements.

As explained in the Definitions section, Education Records are materials "maintained by an educational agency or institution or by a person acting for the agency or institution," and that contain information directly related to a student. However, the definition of "Education Records" is subject to certain exceptions. The following are **NOT** considered Education Records:

- Records kept by the person who made them that are used only as a "personal memory aid" and not disclosed to anyone, except a temporary substitute
- Records maintained by an educational agency's law enforcement unit
- Employee records made in the normal course of business that pertain only to the individual's employment and that are not used for any other purpose
- Records created about a student age 18 or older or who is attending a postsecondary education institution by professionals such as a physician, psychiatrist, psychologist or other recognized professional or paraprofessional acting or assisting in that capacity for treatment of the

student; this information can only be disclosed to those who provide the treatment

- Records that an educational agency created or received after the student stopped attending the institution and that are not directly related to the individual's attendance as a student
- Grades on peer-reviewed papers before they are collected and recorded by a teacher

For more information, see the ED's Protecting Student Privacy While Using Online Education Services: Requirements and Best Practices and National Center for Education Statistics Forum Guide to the Privacy of Student Information.

Education Records: Rights of Parents and Eligible Students:

A key concern of FERPA is ensuring that parents and eligible students—those students who are 18 years of age or older, or are attending a postsecondary education institution—may:

- Inspect and review the student's education records;
- Seek amendment of the student's education records that the parent or eligible student believes to be inaccurate, misleading, or otherwise in violation of the student's privacy rights;
- Consent to disclosures of personally identifiable information contained in the student's education records, except to the extent that FERPA authorizes disclosure without consent; and
- File a complaint with ED concerning alleged failures by the School System to comply with the requirements FERPA.

School Systems are required to advise parents and eligible students of these rights in an annual notice, and must respond to requests to inspect and review the student's Education Records in a "reasonable period of time," upon receipt of the request, not to exceed 45 days. Some state laws impose shorter time frames, so School Systems should be familiar with their state requirements, and have policies and processes in place to respond to these requests in a timely and comprehensive manner. Such policies and processes should include obtaining access to information in the Education Record that may have been disclosed to a Provider, as described below.

Moving From Compliance to Trust:

Maintaining the accuracy and integrity of the data should be part of any School System compliance program. It is critical to earning the trust of parents, students and other community stakeholders.

DISCLOSING STUDENT DATA: FERPA AND THE SCHOOL OFFICIALS EXCEPTION

One of the most common ways in which you may disclose personally identifiable information from Education Records to your employees and Providers is by designating that party as a School Official, as that term is used in FERPA. In order to do that, the person or entity with which you are disclosing information must meet certain criteria.

To decide whether or not the criteria have been met, you must be able to answer "yes" to one or more of the following:

☐ Is the person a teacher or other employee within your educational agency, with a legitimate educational interest in the records you would like to disclose?

☐ In determining whether or not the person has a legitimate educational interest, consider whether or not the intended use for the information is **consistent with what has been disclosed to parents** in your legally required annual notice defining a legitimate educational interest, as well as any School System policies on this matter.

— OR —

☐ Is the person or entity a contractor, consultant, volunteer or other party to whom you have outsourced institutional services or functions?

☐ If so, does the contractor, consultant, volunteer or other party meet **ALL** of the following criteria:

1. They perform an institutional service or function for which you would otherwise use employees
2. They are under your direct control with respect to the use and maintenance of Education Records;
   - In determining whether or not you have "direct control" of how the Provider may use and maintain the Education Records, consider whether or not you have a contract with the Provider that details—in the words of ED—"all of the necessary legal provisions governing access, use and protection of the data." For more on contract fundamentals, see **Contracts and Terms of Service**.
3. They may use the personally identifiable information in the Education Records only for the purpose for which you disclosed it, and for no other purpose unless they first obtain the written consent of the parent or eligible student.*

* *Please keep in mind that your state laws may have additional requirements around redisclosure of personally identifiable information, and you should become familiar with those restrictions to be sure you understand the extent of the legislative landscape.*

You must use what ED refers to as "reasonable methods" to ensure that all of your School Officials are provided with access to only the personally identifiable information in Education Records in which they have a legitimate educational interest. When working with your employees, consider what information they need to know, compared with what information might be convenient for them to have. "Need to know" should be the standard through which you operate.

When working with Providers, they too, must only receive access to the personally identifiable information in Education Records in which they have a legitimate educational interest. In order to assess that, you'll want to review the Provider's Privacy Policy, which should explain what information they collect and why, and how they handle that information. Remember that as a School System, you are not authorized to allow a Provider to use personally identifiable information from Education Records for commercial purposes, only for purposes that serve the legitimate educational interest. As noted above, you also need a contract with the Provider that establishes your "direct control" over how the data is managed, including agreement on what data is disclosed, what it may be used for, how it is secured and how and when it is deleted. You must also use physical, technological and/or administrative controls to ensure that student data is disclosed only to those who have a legitimate educational interest in receiving it.

EXAMPLE OF SCHOOL OFFICIAL AND PERMITTED USES OF DATA

"A district contracts with a Provider to manage its cafeteria account services. Using the ***School Official exception***, the district gives the Provider student names and other information from School System records (not just Directory Information). The Provider sets up an online system that allows the School System, parents, and students to access cafeteria information to verify account balances and review the students' meal selections. The Provider cannot sell the student roster to a third party, nor can it use PII [personally identifiable information] from Education Records to target students for advertisements for foods that they often purchase at school under FERPA, because the Provider would be using FERPA-protected information for different purposes than those for which the information was shared."

MORE INFORMATION: *ED's Protecting Student Privacy While Using Online Education Services: Requirements and Best Practices and Future of Privacy Forum's, Who Is a School Official Anyway?*

Directory Information FERPA Exception

As noted in the flowchart, a School System may disclose Directory Information without obtaining prior consent from the parent or eligible student, as long as the School System notifies the parents or eligible students of the data to be disclosed, and provides the parent or eligible student with a reasonable amount of time to opt out of the disclosure. Directory Information, as defined in FERPA, allows School Systems to conduct some fundamental and often expected practices, such as publishing team rosters, the program for the school play or the student yearbook.

The Definitions section lists the types of information that may qualify as "Directory Information," such as a student name, address, telephone listing, email address, etc.

As noted by the ED, School Systems must: provide public notice of the types of information which they have designated as "Directory Information," give parents or eligible students the right to opt out of that disclosure, and explain the period of time during which the parents or eligible students have to provide written notice to opt out of disclosure of Directory Information.

Limited Release Policy for Directory Information:
Objections to release of Directory Information frequently occur when parents are unclear about who might receive the information, or whether or not it would be disclosed for commercial purposes unrelated to the School System.

One option for a more privacy-friendly approach to Directory Information is the implementation of a limited Directory Information release policy, or both.

Under this type of policy, an LEA can (a) designate the specific entities that may receive Directory Information, (b) designate the specific purposes for which Directory Information may be disclosed, or both.

"An educational agency or institution may specify in the public notice it provides to parents and eligible students in attendance provided under § 99.37(a) that disclosure of Directory Information will be limited to specific parties, for specific purposes, or both."

Examples of School Systems with a limited release policy include:

- Logan-Rogersville R-VIII School District (restrictions on specific data e.g. email)
- Vail Unified School District (limitation to promoting school programs and similar purposes)
- Fairbanks North Star Borough School District

Remember that in adopting a limited release policy for Directory Information, the School System MUST abide by the limitations that it describes in the required annual notice. If a School System wants to disclose data for a purpose not specified in the notice, it must provide parents and eligible students with an additional notice and the opportunity to opt-out of such disclosure.

See National Center for Education Statistics Forum Guide to the Privacy of Student Information for more information.

FREQUENTLY ASKED QUESTIONS ABOUT DIRECTORY INFORMATION

Can a School System use the Directory Information exception to create student accounts in a Provider product if that is the only information required?

The ED points out that while disclosing information with a Provider under this exception may appear to be a good option for School Systems, it has two major drawbacks:

- First, only Directory Information specified in the public notice may be disclosed using this exception.
- Second, the fact that parents and eligible students may, and often do, "opt out" of disclosing their information can create an imbalance in the classroom environment or in administrative systems if some students have been opted out of disclosure while others have not.

Additional risk may ensue if the student will create data through the use of the product that should be treated as part of the Education Record. If the school has not designated the Provider as a "School Official," they may not have direct control over that data.

Lastly, if the Provider collects data from the student and uses that data for marketing purposes, the Protection of Pupil Rights Amendment (PPRA) may apply.

Therefore, the ED suggests that the School Officials exception is likely a better option for School Systems when disclosing information to an online service Provider.

What special precautions do schools need to take regarding categorizing Student IDs as Directory Information?

The 2008 amendments to FERPA allow the categorization of the Student ID as Directory Information when the Student ID is an identifier for electronic systems, AND when the identifier is **combined with other authentication factors known only to the user**, such as a password.

Per ED: "This will prevent districts and institutions from attaching these identifiers to students' names on sign-in sheets in classrooms, health clinics, etc.; prevent schools from disclosing lists with these identifiers attached to students' names, addresses, and other Directory Information; and prevent teachers from using them to post grades."

This is intended to help reduce the risk of unauthorized access to personal information and identity theft by ensuring that schools do not make these identifiers available publicly.

School Officials will still be able to use class lists with ID numbers but cannot make them available to students or parents. Teachers that still post grades publicly will have to use a code known only to the teacher and the student."

This means that Student ID cannot be considered Directory Information when posting grades or other student work, or as the sole means of access to student information or services (e.g. logging in to a website, checking out library books, or paying for lunches).

In order to consider the Student ID as Directory Information, the school must:

- Declare this use in their annual notice AND
- Ensure that it is combined with some other identifier.

As noted above, parents and eligible students may opt out of Directory Information disclosures. When that happens, those students will not be able to participate in Provider services that require a Student ID if the information is disclosed to the Provider under the Directory Information exception of FERPA. (See FERPA Final Rule 34 CFR Part 99 Section-by-Section Analysis December 2008.)

PPRA (Protection of Pupil Rights Amendment) At-a-Glance

The Protection of Pupil Rights Amendment ("PPRA") applies, with some minor exceptions, to data collected directly from the student via any program that receives funding from ED. Generally, PPRA requires School Systems to obtain prior written consent from parents or students over the age of 18 before administering a survey, analysis or evaluation that requires students to disclose any of the following Sensitive Information:

- Political affiliations or beliefs of the student or the student's parent
- Mental and psychological problems of the student or the student's family
- Sex behaviors or attitudes
- Illegal, anti-social, self-incriminating, or demeaning behavior
- Critical appraisals of individuals that have a close family relationship with the student
- Legally privileged or analogous relationships, such as conversations with doctors, lawyers or clergy
- Religious practices, affiliations, or beliefs of the student or the student's parent
- Income (other than information required by law to determine eligibility for financial aid)

If funds from ED are not used for such surveys, but such surveys are conducted with information collected directly from the students, School Systems must still notify parents, at least once at the beginning of the school year, of:

- The date(s) when the surveys may be conducted;
- The right to opt their child out of participating; and
- The right to request for review any instructional materials used in connection with any survey that involves the subject matter noted above and those used as part of the educational curriculum.

These requirements apply regardless of whether or not the School System administers the survey directly or uses a Provider to administer it. However, if a Provider administers the survey on behalf of the School System, contractual clauses should be in place restricting the Provider's use of the information obtained from students only to serve the school purpose.

Development of Policies

Under PPRA, School Systems are also required to work with parents to develop and adopt policies addressing:

- That parents have the right to inspect, upon request, a survey created by a third party before the survey is administered or distributed by a school to students, and the procedure for granting a request by a parent for such access;
- How the School System will protect the privacy of student information in the event that a survey is administered to students that contains subject matter described above, and the right of parents to inspect, upon request, a survey that concerns one or more of the eight protected items of information);
- The right of parents to inspect, upon request, any instructional material used as part of the educational curriculum for students, and the procedure for granting a request by a parent for such access;
- Administration of physical exams or screenings of students;
- The collection, disclosure, or use of personal information (including items such as a student's or parent's first and last name, address, telephone number or social security number) collected from students for marketing purposes, or to sell or otherwise provide the information to others for marketing purposes, including the School System's arrangements for protecting student privacy in the event of collection, disclosure, or use of information for these purposes; and
- The right of parents to inspect, upon request, any instrument used in the collection of personal information for marketing or sales purposes before the instrument is administered or distributed to a student and the LEA's procedure for granting a parent's request for such access.

PPRA does allow School Systems to collect, disclose or use personal information collected from students to develop, evaluate or provide educational products or services for the students or the School System without creating a policy for such practices. Generally, this includes activities such as:

- College or other postsecondary education or military recruitment
- Book clubs, magazines, and programs providing access to low-cost literary products
- Curriculum and instructional materials used by elementary schools and secondary schools
- Tests and assessments used by elementary schools and secondary schools to provide cognitive, evaluative, diagnostic, clinical, aptitude, or achievement information about students (or to generate other statistically useful data for the purpose of securing such tests and assessments) and the subsequent analysis and public release of the aggregate data from such tests and assessments
- The sale by students of products or services to raise funds for school-related or education-related activities
- Student recognition programs

Keep in mind, however, that these rights need to be assessed in conjunction with FERPA and COPPA requirements, as well as state law restrictions. In short, just because something is permissible under PPRA or another law, does not mean that a School System may actually engage in that activity. The full matrix of legislation needs to be considered as a whole, for each use case.

Moving From Compliance to Trust

Despite this exception in the law, consider carefully, and within the context of your entire community ecosystem, if you might sell information collected from students or use it for marketing purposes. As a best practice, develop policies to govern your collection and use of information for sale or marketing purposes, and make these policies available to parents. This will help ensure that parents understand how their children's information is being used, and are not taken by surprise, even if the activity you are engaged in may be legal. Also be sure to consult your state laws which may have restrictions on these activities that go beyond the requirements of PPRA.

Parental Notification and Opt-Out

If a School System participates in any of the following activities, it must notify parents and students age 18 and older as follows:

ACTIVITY	NOTICE
▶ The collection of Personal Information directly from students to use for marketing or to sell to another party	▶ Notify parents and students 18 and older of policies surrounding these activities; be mindful of additional or conflicting state law limitations.
▶ Any survey that asks students to provide Sensitive Information	▶ Request permission from parents prior to providing such surveys to students
▶ Any invasive, non-emergency physical examination or screening that is required as a condition of a student's school attendance, administered by the school and scheduled by the school in advance and not necessary to protect the immediate health and safety of the student or of other students and not required or permitted by state law.	▶ Notify parents and students 18 and older of times and dates when you plan to perform any of these activities

For more information on PPRA as it applies to online contexts, see Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices.

COPPA in Context

Although FERPA leads the way as the key federal law regulating how School Systems manage student data privacy, and the PPRA regulates collection of information from students about sensitive subjects and use of data for marketing purposes, it can be helpful to take a closer look at an equally important federal law that regulates how Providers must protect the privacy of personal information collected directly from children under the age of 13: COPPA.

FIRST, WHICH LAW APPLIES WHERE?

FERPA	PPRA	COPPA
▶ Applies to School Systems that receive funding from ED. The Provider should align with FERPA and work with the School System to ensure that their product or service may be used in compliance with FERPA.	▶ Applies to School Systems that receive funding from ED. The Provider should align with PPRA and work with the School System to ensure that their product or service may be used in compliance with PPRA.	▶ Applies to operators of commercial websites and online services that are directed to children under 13 and that collect, use, or disclose personal information from children under 13, or that have actual knowledge that they are collecting personal information from children under 13, either directly or from users of another website or online service directed to children under 13. The Provider may rely on a contract with a School System, including a click-wrap agreement, to indicate that the School System has obtained the necessary parental consents to collect the data. However, the Provider must supply the school system with advance notice of its information collection, use and disclosure practices, so that the School System may make an informed decision. (See FTC's Complying With COPPA Frequently Asked Questions.)

The truth is that at any given time, any or all of the laws may apply. While the flowchart takes you through a decision tree about FERPA, COPPA and PPRA, it's equally important to understand that the laws are not mutually exclusive.

WHAT DATA IS PROTECTED?

FERPA	PPRA	COPPA
▶ Education Records, including data collected from and about parents and students.	▶ Data collected by a School System or Provider from students about specific, sensitive subjects or to develop, evaluate or provide educational products or services as described above.	▶ Personal information collected online from children under the age of 13.

Regardless of the law, parents retain certain rights around the collection, use and disclosure of their child's data. Some of these are listed here:

FERPA	PPRA	COPPA
▶ Right to review the student's Education Record and request amendment of mistakes. Must consent to disclosure of their child's personal information, unless that information is sent to a Provider or other party operating as a designated School Official. Right to opt out of disclosure of what a School System has designated as Directory Information.	▶ Right to review surveys or similar materials requesting information from students about specific, sensitive subjects and opt their child out of participating. Must be part of policy development related to access to the materials referenced above, instructional material related to the curriculum, administration of physical exams and marketing prohibitions, with certain limited exceptions.	▶ Must consent to collection, use and disclosure of their child's personal information prior to collection except in limited circumstances. Right to review information collected from their child, request that it be deleted and/or request that no additional personal information be collected from their child.

When working with Providers, **be sure you consider all of these laws**, as well as your state student data privacy laws, which may include additional requirements and restrictions.

NAVIGATING FEDERAL LAWS: GETTING STARTED

Some questions to consider:

- ☐ Who is collecting the information? Is it the School System or the Provider?
  - » If it is collected by the School System, consider FERPA and PPRA
  - » If it is collected by the Provider, consider FERPA, PPRA and COPPA
- ☐ Is the information being collected directly from the student?
  - » If so, consider FERPA and PPRA
    - ▪ Is the student under age 13?
      - ◆ If so, consider FERPA, PPRA and COPPA
- ☐ Have you obtained parental consent for the use of the data?
- ☐ Is parental consent needed to disclose the data to a Provider?
  - » Who is obtaining the consent, the School System or the Provider?
    - ▪ Remember that the Provider may rely on the School System to obtain parental consent on its behalf only when the student's personal information will be used for the school purposes and not for commercial purposes unrelated to the provision of the services.
- ☐ Will the data be used for marketing purposes authorized by your School System?
  - » Is the use consistent with your school policy?
  - » Have you managed compliance with PPRA?
  - » How have consents been obtained in compliance with COPPA if personal information is to be collected from students under 13?
  - » Have you consulted your state law?

It is an undeniably complex ecosystem, but considering these questions as you assess where and with whom you disclose student data will help ensure that you are properly managing your responsibilities across all legislative requirements.

National Student Lunch Act (NSLA) At-A-Glance

Although not specifically a student data privacy law, the National Student Lunch Act ("NSLA") does contain privacy requirements that are worth noting. The Act established the National Student Lunch Program, which provides free and low-cost lunches to students. At the federal level, the program is administered by the Food and Nutrition Service, and at the state level, it is usually administered by state education agencies through agreements with School System food authorities.

The Program is open to all School Systems—public, nonprofit, private, independent—and as such, the Act requirements apply to all as well.

From a privacy perspective, the Act limits use or disclosure of information obtained from an application for a free or reduced price meal. Such information is only available to:

- A person directly connected with administration or enforcement of the Act,
- A federal education program,
- A state health or education program administered by the State or local educational agency, or
- Certain qualified federal, state or local nutrition programs, the US Comptroller General and local law enforcement investigating compliance.

Even then, the information provided must be limited to income eligibility unless consent is obtained from the student's parent or guardian.

Those who do receive the information are prohibited from disclosing it.

In short, within your School System, knowledge about who is eligible for free and reduced meals must be strictly limited, and care should be taken to ensure that these students are not identified—either directly or indirectly—as participants in the program.

For more information, see 42 USC 1751 and National Center for Education Statistics Forum Guide to Protecting the Privacy of Student Information: Other Federal Laws Affecting Information Privacy in Schools

HIPAA (Health Insurance Portability & Accountability Act) At-a-Glance

The Health Insurance Portability and Accountability Act ("HIPAA") was enacted in 1996 in an effort to set national standards for the transmission of sensitive health information. HIPAA mandates administrative, technical, and physical safeguards to ensure that individual health information remains private and secure. In 2009 the Health Information Technology for Economic and Clinical Health Act (HITECH[1]), part of the American Recovery and Reinvestment Act, incorporated new provisions into HIPAA's Privacy[2] and Security[3] Rules. HITECH established that the Department of Health and Human Services (HHS) would issue guidance regarding technological methods for protecting health information and extended HIPAA enforcement to service Providers or "business associates" who help manage and transmit health information on behalf of a "covered entity."

While HIPAA is important to understand, its application in K12 schools is limited. Most student records, including health records, are Education Records, which are covered by FERPA. As noted in the U.S. Department of Health and Human Services and the U.S. Department of Education's *Joint Guidance on the Application of the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to Student Health Records* (2008) ("Joint Guidance"), "At the elementary or secondary level, a student's health records, including immunization record...as well as records maintained by a school nurse, are Education Records subject to FERPA."[4] This is because these records are often directly related to the student and

1 You can access more information on the HITECH Act at http://www.hhs.gov/ocr/privacy/hipaa/ administrative/enforcementrule/hitechenforcementifr.html

2 You can access more information on the HIPAA Privacy Rule at http://www.hhs.gov/ocr/privacy/hipaa/ understanding/summary/index.html

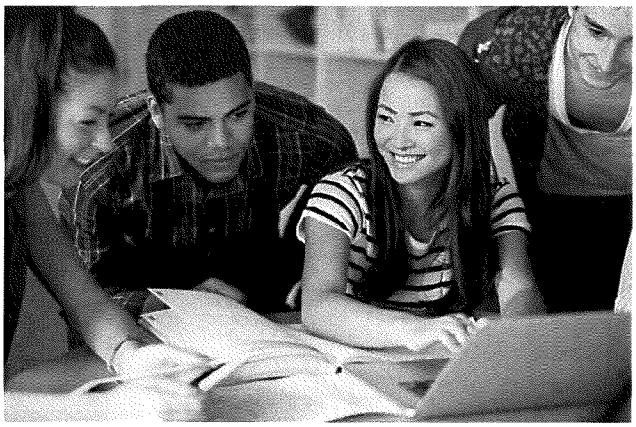
3 You can access more information on the HIPAA Security Rule at http://www.hhs.gov/ocr/privacy/hipaa/ understanding/srsummary.html

4 For more information, see the Joint Guidance on the Application of the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to Student Health Records (2008)

are maintained by the school for its purposes, rather than to process the transactions set forth above.

However HIPAA likely applies to health information related to your School System employees, as well as to the transmission of health information for any of the following purposes:

- Process healthcare claims or equivalent encounter information
- Process health care payments and provide remittance advice
- Coordinate benefits
- Check or process health care claim status
- Enroll or process the disenrollment of individuals in a health plan
- Determine eligibility for a health plan
- Process health plan premium payments
- Certify and authorize referrals
- Process the first report of injury
- Manage and process health claims attachments
- Process health care electronic funds transfers (EFT) and remittance advice



If you are using an online service Provider to transmit your students' protected health information for any of the purposes set forth above, and that information is not part of an education record (as defined by FERPA) then you and your online service Provider need to comply with the obligations and security standards set forth in HIPAA and HITECH. In addition to the contractual provisions covered in **Contracts and Terms of Service,** you should include an obligation to comply with HIPAA, and also have your online service Provider execute a *Business Associate Agreement*[5].

In any event, treating the health information of your students in accordance with the security standards and requirements dictated in HIPAA is generally a good practice, and can be a useful guide to securing your students' information more broadly.

5 For a sample Business Associates Agreement, visit: http://www.hhs.gov/ocr/privacy/hipaa/understanding/ coveredentities/contractprov.html

Vetting Online Tools: **Start with Privacy**

This flowchart will help you understand some of the questions to ask and decisions you need to make when considering your responsibilities under the Family Educational Rights and Privacy Act (FERPA), the Protection of Pupil Rights Amendment (PPRA) and the Children's Online Privacy Protection Act (COPPA).

It does not cover all privacy laws and does not detail all obligations under FERPA, PPRA and COPPA. It is simply a tool to use in getting started. Please check with your legal counsel to understand how federal, state, and local laws may apply to your school.

Application Vetting: An Overview

Understand what data the Provider collects, uses, and discloses, and how the data is protected.

- This can often be done by reading the Provider's Privacy Policy, but in some cases, you may need to examine the product or service.
- Based on the sensitivity of the data and how it is used and disclosed, you may need to get additional details on how the Provider protects the data.

Review the agreements that outline the responsibilities between the Provider and the School System.

- Depending on the service this may be a formal contract, terms of service or "click-wrap" agreement.
- Based on what you have identified in the review of the Privacy Policy, security practices and terms, and any testing you have conducted on the product or service, you may need to negotiate changes or if that is not possible, decide to find an alternative product.

Communicate the decision to teachers, students and parents.

- If the approval comes with any notes, cautions, guidelines or instructions, make sure these are readily available to the approriate stakeholders.
- For parents provide any necessary notice and choice (opt-in, opt-out).

→ Yes → No → Assessment completed

■ Is Student Personally Identifiable Information (PII) Being Disclosed to a Provider?

If YES, consider FERPA, PPRA and any State laws.

- When dealing with Education Records protected by FERPA, parental consent is required unless an exception applies.
- The most common exception is the School Official exception.
- What is or is not an Education Record is always not always clear-cut.
- Be sure to assess whether or not the information being collected, generated, stored or processed by a Provider qualifies as an Education Record with your School System's legal counsel before proceeding.
- Be careful before disclosing data to create student accounts using the Directory Information exception, as the student may create data through the use of the product that should be treated as part of the Education Record.
- Will students be asked to disclose Sensitive Information protected by PPRA?
- Ask the Provider and review the product or service to determine if any other PII is collected (e.g. biometric, geo-location, financial, health)

■ Will the Provider Collect the PII Directly from Students?

If YES, consider PPRA and COPPA.

- PPRA applies when collecting data from students on certain sensitive subjects or when data will be used for marketing purposes.
- COPPA applies when data is collected online by commercial providers from children under 13..

■ Is Parental Consent Required to Disclose PII To The Provider?

If YES, consider PPRA and COPPA.

- PPRA requires parental notification and an opportunity to opt-out when data is collected from students for marketing or sale.
- COPPA consent, for students under 13 is described below

IF the School System is contracting with the Provider and data is used only for the benefit of the students and School System, the school may choose to provide consent on behalf of the parent, and the Provider may rely on the contract as indication that the School System will manage the consents.

OR

IF the Provider collects, uses or discloses data for commercial purposes not related to the provision of the services requested by the school, the school cannot provide consent. Pay attention to any language in terms that prohibit use by children under 13, or delegate responsibility for obtaining consent to the school.

CONTINUED ON NEXT PAGE

■ Will the PII be used for Marketing Purposes, and not for the School Purpose?

Keep in mind that this is a case where the School Official exception would not apply, so consider...

- Is the use consistent with your school's written policy?
- Have you managed any compliance required by PPRA?
- Have you consulted your state law?
- Has the Provider managed COPPA compliance if the information was collected from students under the age of 13?

■ Does the Provider's Privacy Policy Provide Clear Information About Collection and Handling of PII?

- What PII is collected (from the School System and from students)?
- Is PII collected by, or disclosed to 3rd Parties?
- How is the data used?
- How is the data protected?
- How long is the data retained?
- How does the School System access its data?
- What happens to the data when the contract ends?
- Is notice given before changes are made to the Privacy Policy?

■ Does the Provider's Privacy Policy, Terms (or Contract) Provide Sufficient Assurances to Make an Informed Selection?

If YES, communicate the decision to teachers, students and parents.

- If the approval comes with any notes, cautions, guidelines or instructions, make sure these are readily available.
- For parents provide any necessary notice and choice (opt-in, opt-out).

If NO, you may need get additional information, negotiate changes to the contract directly or through an addendum, or if that is not possible, decide to find an alternative product.

COSN Protecting Privacy in Connected Learning

Section 2: Partnering with Providers

Section one of this Toolkit provides an overview of the most common federal laws with which School Systems and Providers must comply. Section two provides guidance on how School Systems should approach applying that information to evaluation of online educational products and services.

Vetting Online Educational Services

The process of vetting online educational products and services is a risk management activity that typically involves four steps:

1. Understand what data the Provider collects, uses, and discloses, and how the privacy of that data is protected. This can often be done by reading the Provider's Privacy Policy, but in some cases, you may need to examine the product or service.
2. Based on the sensitivity of the data being disclosed and how it is used, you may need to request additional details on the Provider's security practices.
3. Review the agreements that outline the responsibilities between the Provider and the School System. Depending on the product or service, this may be a formal contract, terms of service or a "click-wrap agreement." Based on what you have identified in the review of the Privacy Policy, security practices and terms, and any testing you may have conducted on the product or service, determine whether or not you need to negotiate new or additional terms with the Provider.r If that is not possible, find an alternative product or service.
4. Communicate the decision to teachers, students and parents.
    a. If your decision to move forward with a product or service comes with any cautionary notes, guidelines or instructions limiting how it is to be used within the School System, make sure these are readily available to the appropriate stakeholders.
    b. For parents, provide any necessary notice and choice (e.g., opt-in, opt-out).

When evaluating the use of student data against the potential risks, it is helpful to consider the categories of data an application uses, the source of the data and sensitivity of the data.

Categories of data: Education Records, as well as sub-categories of Education Records, such as Directory Information, financial, behavioral, medical, socio-economic, biometric, and other data.

Sources of Data: Data may be disclosed through a variety of sources:

- By the School System administrator (to create the account)
- By the teacher (e.g., class roster, grades, comments)
- By the student (e.g., registration information, responses to questions in an application, etc.)
- By the Provider about students' use of the product or service
- By and to a Provider's 3rd party (e.g., to facilitate delivery of the product or service by the Provider)

Sensitivity: Not all products and services use highly sensitive data, and some School Systems have developed **Data Classification** frameworks to provide guidance when evaluating the risk of disclosing data to a Provider. Developing a classification system also helps to inform the levels of protection that a School System should have in place around the data it has on hand.

> **Data Classification** is the process of assigning a level of sensitivity to categories of data that results in the specification of controls for each category. Having a data classification system enables the adoption of policies and procedures to protect it. (See ISACA Glossary of Terms)

How to Read a Privacy Policy

A Privacy Policy (sometimes called a privacy notice) is used to inform the users of a service what personally identifiable information the Provider collects and how it is collected, used, managed, stored, disclosed and retained. The Privacy Policy is a legal requirement. It must be truthful, and accurately reflect the data practices. The Provider could be subject to regulatory action under Section 5 of the Federal Trade Commission Act if the Privacy Policy is misleading or deceptive.

Here's a list of questions to consider when reading a Privacy Policy. As always, the Privacy Policy should be read in conjunction with any terms of service, "click-wrap" agreement or contract to ensure that you understand the full scope of the Provider's representations about the product or service and data used. Note that not every Privacy Policy will include all of this information, however a fundamental understanding of all of these elements is recommended before you move forward with a Provider.

CONSIDERATIONS WHEN REVIEWING A PRIVACY POLICY

QUESTIONS	EXPLANATION
General Questions • Is the policy easy to find and available before the service collects any user information? • Is it clear which services are covered by the policy? • Does the policy state when it was last updated? • Is it written in a clear and understandable manner?	The Privacy Policy should be available in advance of any decision to use the product, and should be available to all users. It should be clear what products and services it applies to, and should identify when it was last changed. While there are sometimes areas of a Privacy Policy that may be stated in legal language, as with all legal documents, be sure you understand it before agreeing to it.
What Personally Identifiable Data is Collected? • What personally identifiable data is disclosed to the vendor from the School System (e.g., to create accounts)? • What personally identifiable data does the Provider collect from users? • What, if any, metadata* is collected or generated by the vendor, either directly or by third parties through technologies such as via cookies, plug-ins, ad networks, web beacons, etc.?	The Privacy Policy should explain what personally identifiable information is collected and how. (For example, is the personally identifiable information provided by the School System, the individual user, or collected passively through the use of various technologies?) **Note that sometimes metadata is not personally identifiable.*

QUESTIONS	EXPLANATION
How is the Data Used? • Does the Privacy Policy explain how the Provider may use data from the School System and your students? • Does it specify any limits that may apply to the Provider's use of that data? • Does the Privacy Policy make it clear that the Provider will only collect, store and use personally identifiable information as necessary to perform the designated services for the School? • If applicable, does the policy address how sensitive information such as fine geolocation data, might be used?	Fundamental to your maintaining "direct control" over the Education Record as required under FERPA, is establishing what data a Provider will have access to, for what purposes and how they may handle it.
Is/How is Data Disclosed? • Does the Privacy Policy specify what data or types of data might be disclosed to 3rd parties? • Does the Privacy Policy provide an explanation of the types of third parties that might receive that data? • Does the Privacy Policy explain what those 3rd parties may do with the data?	In some cases, the Provider may be disclosing information to third parties solely to provide your School System with the product or service you've requested. For example, a Provider may disclose information with a cloud service provider to store the data, or with an analytics company to develop reports to show teachers how their students are progressing in the product. In other cases, the intended use may go beyond that legitimate educational interest or fundamental operation of the product. Consider if the contract needs to clarify whose responsibility it is (the Provider's or the School System's) to obtain parental consent when the intended use may go beyond that legitimate educational interest or basic product operation.

QUESTIONS	EXPLANATION
Data Access • Does the Privacy Policy specify whether the School System and/or parents (or eligible students) will be permitted to inspect and request to amend records as specified in FERPA? • If access to inspect the records is not available directly to the School System and/or parents (or eligible students), does the Privacy Policy explain how the Provider will facilitate such access if requested? • Does the Privacy Policy make it clear what the process would be to obtain such access?	Under FERPA, School Systems are required to respond to requests from parents and eligible students to inspect and request to amend certain information in the Education Record. Be sure you understand how you will manage such requests when the data is held by a Provider.
Data Security • Does the Privacy Policy provide basic information about the data security practices? • Based on the Data Classification of the information stored and any associated risks, does the Privacy Policy specify any security requirements that the Provider would follow to the extent that it maintains, processes, or stores that information on behalf of the School System?	Consider whether or not the Privacy Policy notes that the security practices are consistent with standard industry practices or commercially reasonable measures. If you have specific security requirements for your data, assess whether or not these considerations are addressed in the Privacy Policy, terms, click-wrap or formal contract.
Data De-identification • Does the Privacy Policy explain if the Provider will de-identify data, and what that de-identified data will be used for? • Does the Privacy Policy include language that indicates an understanding of the FERPA de-identification standard?	It is fairly common for Providers to want to use de-identified data. FERPA has a very high standard for de-identification, and you may want to consider whether or not the Provider's Privacy Policy, terms, click-wrap or formal contract refers to that standard. In addition, many state laws restrict the use of de-identified data to specific purposes. Refer to your state laws to ensure that the Provider's use cases align with your understanding of the regulatory requirements.

QUESTIONS	EXPLANATION
Data Retention and Disposal. • Does the Privacy Policy address how long the data will be maintained? • Does the Provider intend to retain de-identified data?	Personally identifiable data disclosed to the Provider, or collected by the Provider during the use of the product or service should be disposed of by secure means within a reasonable time frame to ensure that it is protected from unauthorized access or use. (See PTAC's Best Practices for Data Destruction) Consider any state or local records retention laws or policies, which may have specific requirements about when data must be deleted. In addition, some recent state laws give students certain rights to keep their user-generated data if the Provider maintains user accounts. You should also understand whether or not de-identified information will be retained.
Changes • Will the Provider give notice and provide the opportunity for the School System to consent before making material changes to the Privacy Policy?	"Material" change is a legal question, but it commonly refers to changes that involve using or disclosing data in a new way, different from the original purpose for which it was collected, or changes that adversely impact the privacy or security of the data. Under these circumstances, the Provider is legally required to provide notice and obtain consent to the changes. Non-material changes may include changing the Privacy Policy to make it easier to read, improving privacy and security protections or explaining a new feature that does not include using already collected data in a new way. These types of changes generally require notice, but not consent.
Contact • Does the Privacy Policy provide a contact for privacy related questions?	Be sure you understand how you can contact the Provider if you have questions about the Privacy Policy.

Understanding Metadata and De-identification

Many Providers collect contextual, transactional or log data as part of their operations, often referred to as '**metadata**.' In the broadest terms, metadata is simply information about a data set. **It may or may not** contain information that identifies an individual.

Examples of metadata that a Provider may gather without identifying an individual might include how many users visited their product or service, what pages within the product or service were viewed, how much time an individual spent answering a question or at what times of day the product or service was accessed. This is all useful information about how a product or service is used, whether or not certain pages are more popular than others, if there may be areas of the product that are difficult to use, if there are technical issues with a certain section of the product or service, what times of day the Provider should be prepared to handle high volumes of user traffic or even, in the event of a security issue, exactly when the incident occurred. It can be critical information to the development and maintenance of a product.

However, in some cases, metadata may be linked to other information, and that combination of information may identify a student. In those instances, metadata must be treated in the same manner as all other types of personally identifiable information, unless and until all information linking metadata to a student has been removed.

De-identifying data refers to the process of removing all personally identifiable information, such that the remaining information does not reveal the identity of an individual.

As noted in the **FERPA Definitions** section, FERPA considers de-identified data to be data from which all personally identifiable information has been removed, and a reasonable determination made that a student is not personally identifiable, whether through single or multiple releases of information, and taking into account other reasonably available information.

Once the data has been de-identified, the ED notes that both School Systems and Providers may release it without parental consent.

However, the standard for de-identification under FERPA is quite complex, and whether or not data is considered to be de-identified may change, depending on how different data elements may be combined. In that sense, de-identification of data under FERPA is both an art and a science. Before you disclose de-identified data, consider engaging with competent experts to review your de-identification standards.

In addition, ED's Chief Privacy Officer Kathleen Styles cautions, "re-identification risk is a very real risk. You can't just take off somebody's name and say that the record is anonymized. With the amount of information that's available online, it's increasingly easy to re-identify individuals." One way to address this would be to include clauses in Provider contracts to exclude rights to re-identify data.

There is also sometimes a good deal of confusion about **aggregated data**, a term which is sometimes used—incorrectly—as synonymous with "de-identified data." **Aggregated data** is simply a collection of data. It may or may not be identifiable. However, you should not consider "aggregated" data to be "de-identified" unless it is specifically described as "aggregated, de-identified data."

For more information, see ED's Protecting Student Privacy While Using Online Education Services: Requirements and Best Practices.

Security Questions to Ask of an Online Service Provider

Security deals with the preservation of confidentiality, integrity and availability of information. It is important to understand your Provider's security practices to ensure that data disclosed to and collected by the Provider remain confidential and protected.

> While most privacy laws do not prescribe specific security standards, regulatory guidance often refers to "reasonable security methods." According to ED, methods are usually considered reasonable "if they reduce the risk to a level commensurate with the likely threat and potential harm." The greater the harm that would result, the more protections a school or district must use to ensure that its methods are reasonable. (See FERPA Final Rule 34 CFR Part 99 Section-by-Section Analysis December 2008.)

School Systems should work with their security representative and look to industry suggested practices when assessing an online service Provider.

The following is a non-exhaustive list of key security questions to discuss with your Provider.

Network Operations Center Management and Security

- Does the Provider perform regular penetration testing, vulnerability management, and intrusion prevention?
- Are software vulnerabilities patched routinely or automatically on all servers?
- Are all network devices located in secure facilities and under controlled circumstances (e.g., where access is managed via ID cards, entry logs, etc.)?
- Are backups performed and tested regularly and stored off-site?
- How are backups secured? Disposed of?

Data Storage and Data Access

- Where will the information be stored and how is data "at rest" protected (i.e. data in the data center)?
  - » Will any data be stored outside the United States?
  - » Is all or some data at rest encrypted (e.g., just passwords, passwords and sensitive data, or all data) and what encryption method is used?
- How is the data protected in transit? (e.g., TLS, SFTP, HTTPS)
- How will the information be stored? If the cloud application is multi-tenant (several districts on one server/instance) hosting, how is data and access separated from other customers?
  - » Records for a School System must be maintained separately, and not be mingled with data from other School Systems or users. That does not mean that a multi-tenant solution can't be used, however you will want to ensure that technical or physical separation is provided.
- Are the physical server(s) in a secured, locked and monitored environment to prevent unauthorized entry and/or theft?
- Who has access to information stored or processed by the Provider?
  - » Under FERPA, individuals employed by the Provider may only access school records when necessary to provide the service to the School System.
  - » Does the Provider perform background checks on personnel with administrative access to servers and School System data?
- What is the Provider's process for authenticating callers and resetting access controls, as well as establishing and deleting accounts?

Availability

- Does the Provider offer a guaranteed service level?
- What is the backup-and-restore process in case of a disaster?
- What is the Provider's protection against denial-of-service attack?

Audits and Security Standards

- Does the Provider give the School System the ability to audit the security and privacy of its records?
- Have the Provider's security operations been reviewed or audited by an outside group?
- Does the Provider comply with a security standard such as the International Organization for Standardization (ISO), and the Payment Card Industry Data Security Standards (PCI DSS) for specific types of data?

Data Breach, Incident Investigation and Response

- Has the Provider agreed to inform you in a timely manner of a breach involving your data, in compliance with applicable laws?
- Will the Provider notify, or assist you in notifying, any affected individuals in compliance with applicable laws?
- Will the Provider assist you by providing a clear explanation of any such incident, including providing you with documentation on the root cause, scope, mitigation and steps taken to ensure protections in the future?

Contracts and Terms of Service

After you have completed your review of a Provider's product or service, Privacy Policy and security practices, it is important to engage with a contract that specifies how the Provider will manage their responsibilities including compliance with laws and your School System's privacy and security requirements.

Drafting or agreeing to a contract should be done under the guidance of your School System's legal counsel; however, the following suggested contractual terms identify key components to consider.

CONSIDERATIONS FOR CONTRACTS AND TERMS OF SERVICE

TOPIC	EXPLANATION
Purpose. Describe the purpose of the product or service being provided. If applicable, specify that the Provider is designated as a School Official, describe the legitimate educational interest that the Provider is fulfilling, describe the nature of the data collected, and the purpose for which any personally identifiable information from Education Records is being disclosed.	If you have determined that the Provider qualifies as a "school official" under FERPA, this establishes the conditions under which you are disclosing the personally identifiable information from Education Records. This summary description may also be useful in writing a notice to parents about the online services used by the school.
Contract Scope. Identify all elements that comprise the agreement and any contract terms that are incorporated by reference (e.g. the Provider's Privacy Policy) and what order of precedence is followed in the event of a contradiction in terms.	A Provider's terms (or the products themselves) may contain links to documents that could be updated over time, and/or may contain language that contradicts the agreement between the Provider and the School System. Defining the order in which terms are to be interpreted, when applicable, reduces the potential for misinterpretation.
Data Collection, Use and Transmission. Specify how the Provider may use or collect data from the School System and your students, and any restrictions that may apply to the Provider's use of that data. Be clear that the School System, and not the Provider, retains control over and rights to the personally identifiable student data.	Fundamental to your maintaining "direct control" required under FERPA is establishing what data a Provider will have access to, for what purposes and how they may handle it. Some or all of this may already be contained within the Provider's Privacy Policy, and that can be helpful if it is incorporated into the agreement by reference. However there may be items missing or additional details that should be added to the agreement.
Data De-Identification: Specify if a Provider may de-identify any of the data and if it will retain such de-identified information.	Consider your state law allowances and restrictions on a Provider's use of de-identified data.

TOPIC	EXPLANATION
Data Security. Specify any security requirements that the Provider must follow to the extent that it maintains, processes, or stores personally identifiable information on behalf of the School System. At a minimum, the contract should specify: • That the Provider securely maintains all such records or data either received from the School System or collected directly from the school, teachers, students, or parents in accordance with industry standards. • That the Provider restricts access to your School System's personally identifiable information to only those individuals that need to access the data in order to perform the agreed-upon services. In addition, if you require that specific security standards must be in place for certain data elements, those should also be specified in the agreement **if** those data elements will be disclosed to the Provider. *See* **Vetting Online Educational Services**. Clarify whether or not you may audit the security and privacy of your School System's or students' personally identifiable information, or have access to results of third party audits. Require notification about changes that will adversely impact the availability, security, storage, usage or disposal of any information. Data collected and stored from and on behalf of one School System should be stored and maintained separately—either by physical or technical means—from the information of any other School System.	Ensure that the contract provides appropriate assurances about how your School System's personally identifiable information will be protected, in alignment with your School System policies and relevant to the data that the Provider will receive or collect.
Data Breach: The agreement should identify what happens if the Provider has a data breach that impacts your School System information. The agreement should identify the Provider's responsibilities including required notification time, and any obligations for end user notification and mitigation.	The procedures should, at a minimum, follow the legal requirements, which vary by state. Most states have data breach laws dealing with financial and other sensitive information, and some have laws addressing breach of education data.

TOPIC	EXPLANATION
Data Retention and Disposal. Assure the proper management and disposal of personally identifiable student and employee data. All personally identifiable data disclosed to the Provider, or collected by the Provider, must be disposed of by secure means to ensure that it is protected from unauthorized access or use. Keep in mind that some School System information may need to be retained for the Provider's legal record-keeping purposes, but that should not include student information.	Consider any state or local records retention laws or policies, including rights that students may have under certain state laws to retain copies of their user-generated content in the event that the Provider supports student accounts.
Bankruptcy or Acquisition. Specify what happens to the data if the Provider goes out of business or is acquired by another organization.	Consider if the data will remain protected under the agreed-upon contract, Privacy Policy and security policy if the vendor is acquired, or merges with another organization, or in the event of bankruptcy or dissolution.
Service Levels and Support. Specify the service levels the Provider must meet and any credits you will receive for any failure by the Provider to meet those service levels. Require the Provider to supply the School System with the technical assistance you may need to operate the services.	Service Level agreements deal with expectations of availability, which along with integrity and confidentiality, is one of the three key principles of security.
Governing Law and Jurisdiction. Typically a Provider's default contract will specify that it is governed by the law of the Provider's home state. Public institutions generally have significant restrictions on their ability to consent to such provisions under the School System's local state laws.	Check with your legal counsel about what law can govern contracts entered into by your School System in light of your state laws.
Duration, Modification and Termination. Establish for how long the agreement will be in force, and what the procedures will be for modifying the terms of the agreement (mutual written consent to any changes is a best practice). Specify what both parties' responsibilities will be upon termination of the agreement, particularly regarding disposition of student information maintained by the Provider. Upon termination of the contract, the Provider should return all personally identifiable student information or allow the School System to download that data, and properly delete any copies still in its possession, including archives and/or backups.	Agreements should govern behavior during and at the end of the term. In addition, allowing one party to modify an agreement at will puts the other party at a legal disadvantage and may jeopardize a School System's ability to retain control over the student data as required by FERPA.

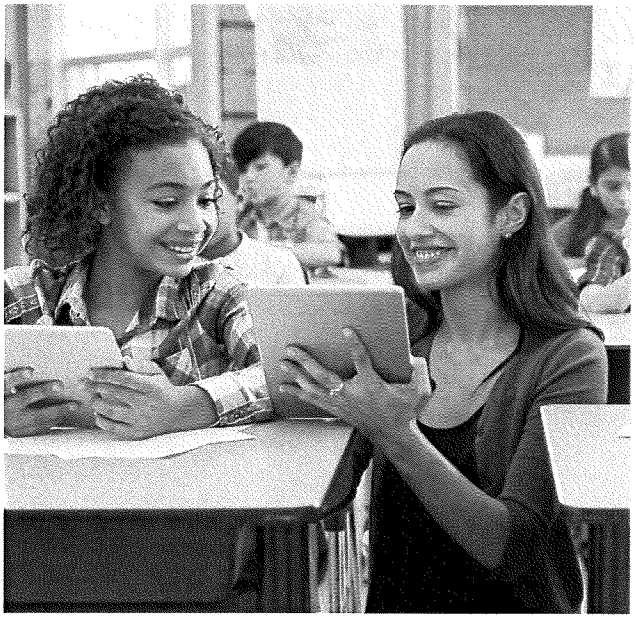
TOPIC	EXPLANATION
Liability. The Provider should be responsible for the activities of its staff and subcontractors. Both parties should have an obligation to comply with all applicable laws, including applicable state student data privacy laws, and each party should be liable for its own actions. If the Provider will be collecting data from children under the age of 13, the Provider should comply with COPPA.	Avoid being too broad. It is unrealistic to stipulate that a Provider comply with the entire state education code, or other laws or sections of laws that do not apply. It is similarly unrealistic to stipulate that a Provider assume liability for data breaches or other incidents caused by the School System. Limits of liability should appropriately allocate risk between the Provider and the School System as the owner of its data.

See also FTC's Start with Security: A Data Security Guide for Schools and the National School Boards Association Data Security Guide for Schools.

Due Diligence for "Click-Wrap" Software

If a teacher, administrator or other employee of the School System clicks through a Terms of Service agreement (often referred to as "click-wrap" agreements) to gain access to technological tools, those actions can bind the School System to terms that may not align with security protocols, district policies, and applicable privacy laws, especially in the case of Providers who are not otherwise aware that their product is being used in an education environment. This can put the School System at legal risk. It is important to develop a procedure for assessing Providers' contracts—including click-wrap agreements—to ensure that they meet your requirements.

Regardless of the form that a contract may take, if the school is sharing Education Records, FERPA requires that School Systems maintain **direct control** over the data. To that end, the ED recommends that "free online educational services go through the same (or a similar) approval process as paid educational services to ensure that they do not present a risk to the privacy or security of students' data."



Understanding that it may not be practical, or even possible, for your School System to negotiate with every Provider makes it more likely that someone at your School System may want to onboard a technology that is available under a "click-wrap" agreement. Consider ways to streamline the contracting process while still managing your risk, so that selecting an online service Provider does not adversely impact acquisition of robust tools that could benefit the students in the classroom.

For example, you might establish a policy that designates which employees in your School System are authorized to click through Provider agreements. Although there are no existing federal requirements as to who in a School System may contract with Providers, most school districts already have such policies for paid services. When it comes to COPPA, the FTC recommends that, as a best practice, the decision about whether or not a Provider's information practices are appropriate should be made at the district or school administration level, rather than delegating it to a teacher, noting

that many schools have a process for assessing Provider practices so that the task doesn't fall on a teacher's shoulders.

With the policy in place, provide adequate information and training to these individuals so that they can make informed decisions in evaluating the services and agreements. Establishing such a policy can also be useful in providing parents with notice of how the district designates a School Official under FERPA.

Ensure that the Provider is obligated to maintain the privacy of your students' data and that these click-wrap agreements otherwise meet the requirements of applicable federal and state laws. As with more formal written contracts, the terms of click-wrap agreements shouldn't be modified without mutual written consent. Consider printing or creating a digital copy of "click-wrap" agreements. This will provide you with a record of the terms that you agreed to at that time, just as you would have with a written contract.

This process should also include guidelines and training for when a contract or contract rider may be required in addition to the click-wrap agreement. When School System requirements are missing from an agreement, School System legal counsel may create a rider in the form of a Data Sharing Agreement or Confidentiality Addendum, containing the School System's minimum requirements and obligations that Providers will need to sign before the School System can utilize the services. In using this approach, however, School Systems should keep in mind that every situation is different and it is unlikely that a single rider will work in every situation without some negotiation.

Ten Steps Every District Should Take Today

With so much uncertainty about what districts can or should be doing to help protect the privacy of student data, it can be easy to lose sight of some very concrete steps that can be taken today.

1. **Designate a Privacy Official**—A senior district administrator needs to be designated as the person responsible for ensuring accountability for privacy laws and policies. The work of implementing and ensuring compliance must be collaborative, and will cut across many departments, but someone needs to be in charge.
2. **Seek Legal Counsel**—Make sure that the legal counsel used by your district has access to and understands education privacy laws and how they are applied to technology services. Do not wait until there is a pressing issue that needs to be addressed.
3. **Leverage Procurement**—Every bid or contract can include standard language around a wide range of legal issues. By adopting standard language related to privacy and security you will make your task much easier. However, many online services are offered via "click-wrap" agreements that are "take it or leave it." You may have to look for alternative solutions or negotiate a rider with the vendor if the privacy provisions of those services do not align with your expectations.
4. **Know the Laws**—Many organizations have published privacy guidance for schools, such as this Toolkit. The US Department of Education's Privacy Technical Assistance Center is a must-know resource at http://ptac.ed.gov/.
5. **Adopt School Community Norms & Policies**—Beyond the privacy laws, what does the school community really expect when it comes to privacy? Seek consensus regarding collecting, using and sharing student data.
6. **Implement Workable Processes**—There must be processes in place for selecting instructional apps and online services. No one wants to slow innovation, but ensuring privacy requires some planning and adherence to policies. Once enacted, the policies should be reviewed regularly to ensure that they are workable and that they reflect current interpretations of privacy laws.
7. **Provide Training**—Staff need training so they will know what to do to protect student data privacy and why it is important. Annual training should be required of any school employee that is handling student data, adopting online education apps and contracting with service Providers. Privacy laws represent legal requirements that need to be taken seriously.
8. **Inform Parents**—Parents should be involved in the development of privacy norms and policies. Just as schools provide information about online safety and appropriate use, they need to put significant effort into making sure that parents understand how schools use student data, and the measures taken to protect student privacy.
9. **Make Security a Priority**—Privacy and security go hand-in-hand. Secure the device, the network and the data center. Toughen password policies. Confirm that your data retention policies align with state legal requirements. Monitor your network for threats. Have regular security audits conducted by a third party expert.
10. **Review and Adjust**—Stay informed about guidance issued by ED and other regulatory authorities to help inform application of privacy laws, and about new laws that may be introduced. Keep your school policies and practices updated to reflect legal requirements and community norms.

Excerpted from Making Sense of Student Data Privacy (May 2014), authored by Bob Moore, Founder, RJM Strategies LLC and supported by Intel. The full report can be found at http://www.k12blueprint.com/privacy.

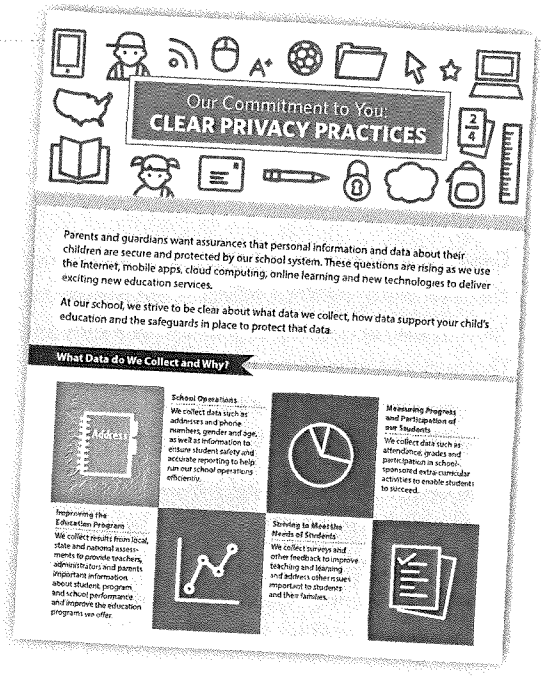
Disclaimer: CoSN is a professional association comprised of school system technology leaders, not lawyers. While we aim to provide valuable tools to help you navigate these issues, you should not rely solely on these tools for legal advice. In all circumstances, please seek appropriate legal or other professional advice regarding specific facts and circumstances pertaining to your school system. This document does not cover all privacy law or policy. You should always consult your legal counsel to understand how federal, state, and local laws and policies may apply to your school system.

Communicating with Parents

Parents and community members are justifiably anxious when it comes to privacy in schools, and it can be challenging to find the right place to start that conversation with parents in your community. CoSN and the National School Public Relations Association (NSPRA) teamed up to produce an infographic that empowers school leaders to discuss the critical issue of student privacy. The infographic breaks down what's important and helps to demystify the issues by allowing you to provide customized answers to questions such as:

- What data is collected and why?
- How does education data support student success and school improvement?
- How is education data protected?

The infographic is available in English and Spanish. For a version that can be customized for your School System, please visit www.CoSN.org/Privacy.



Putting it Together: Moving from Privacy to Trust

The Trusted Learning Environment (TLE) Seal is a mark of distinction for School Systems that have met a rigorous set of standards and demonstrated their commitment to protecting student data and privacy. It was created by CoSN along with 28 School System leaders and lead partners AASA (School Superintendents Association), ASBO (Association of School Business Officials) and ASCD. It encompasses five practice areas that go beyond legal compliance: Leadership, Business, Security, Professional Development and Classroom.

By earning the TLE Seal, School Systems signal to parents and communities that they are serious about protecting student data privacy and have taken concrete, proactive measures to move beyond compliance to foster a trusted learning environment.

For more information about the Trusted Learning Environment Seal Program, including to download the practice requirements, visit www.TrustedLearning.org.

Disclaimer: CoSN is a professional association comprised of school system technology leaders, not lawyers. While we aim to provide valuable tools to help you navigate these issues, you should not rely solely on these tools for legal advice. In all circumstances, please seek appropriate legal or other professional advice regarding specific facts and circumstances pertaining to your school system. This document does not cover all privacy law or policy. You should always consult your legal counsel to understand how federal, state, and local laws and policies may apply to your school system.

Useful Links

Understanding the Laws

- The Privacy Technical Assistance Center (PTAC) http://ptac.ed.gov/ The U.S. Department of Education has established the Privacy Technical Assistance Center (PTAC) as a "one-stop" resource for education stakeholders to learn about data privacy, confidentiality and security practices related to student-level longitudinal data systems.
- *The Family Policy Compliance Office (FPCO) FE*RPA guidance and information https://ed.gov/policy/gen/guid/fpco/ferpa/index.html
- Complying with COPPA: Frequently Asked Questions, FTC http://www.business.ftc.gov/documents/0493-Complying-with-COPPA-Frequently-Asked-Questions
- An Overview of the Children's Online Privacy Protection Act and the Family Educational Rights and Privacy Act, Harvard Law School's Cyberlaw Clinic http://papers.ssrn.com/sol3/papers.cfm?abstract_ id=2354339
- Cheat Sheet: Data Privacy, Security, and Confidentiality, Data Quality Campaign http://www.dataqualitycampaign.org/find-resources/cheat-sheet-data-privacy-security-and-confidentiality

Security

CoSN Initiatives: Cyber Security for the Digital District http://www.cosn.org/cybersecurity

CoSN Member Only Resources Available At cosn.com

- » Security and Privacy of Cloud Computing
- » Webinar: Is Privacy in the Cloud Possible?
- » Cloud Computing: A Billowing Virtual Infrastructure for Services and Savings

- Security Guidance for Critical Areas of Focus in Cloud Computing V3.0, Cloud Security Alliance (CSA) https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf
- Data Security for Schools: A Legal and Policy Guide for School Boards—https://www.nsba.org/data-security-schools-legal-and-policy-guide-school-boards#sthash.oiENdUWM.dpuf

Contracting

Privacy and Cloud Computing in Public Schools, Fordham University http://law.fordham.edu/center-on- law-and-information-policy/30198.htm

Privacy Attitudes

Parents, Teens, and Online Privacy. Pew Research Center's Internet Project http://pewinternet.org/Reports/2012/Teens-and-Privacy.asp

Teens and Mobile Apps Privacy, Pew Research Center's Internet Project http://www.pewinternet.org/2013/08/22/teens-and-mobile-apps-privacy/

Beyond One Classroom: Parental Support for Technology and Data Use in Schools, Future of Privacy Forum https://fpf.org/wp-content/uploads/2016/12/Beyond-One-Classroom.pdf

Training, Education and Communication

CoSN's Protecting Student Privacy in Connected Learning Facilitated Online Course http://www.cosn.org/onlinecourses

PTAC Guidance Videos http://ptac.ed.gov/ptac-guidance-videos

PTAC FERPA 101 Training Videos (log in required) http://ptac.ed.gov/

Putting it Together—Moving from Privacy to Trust

CoSN's Trusted Learning Environment Program http://trustedlearning.org/

Acknowledgements

Version 3 of the CoSN Protecting Privacy in Connected Learning was developed by:

Linnette Attai, President, PlayWell, LLC

Jim Siegl, Technical Architect, Fairfax County Public Schools

Reg Leichty, Foresight Law + Policy

Design by DeGarmo Creative

History of this Work

Since 1992 CoSN has been working with education technology leaders to develop practical resources that help school technology decision makers provide the kind of leadership their School Systems need, so that students can experience technologically-rich learning environments.

In 2013 CoSN released the EdTechNext report on Security & Privacy of Cloud Computing. This document framed many of the privacy issues that School System leaders face and is a good first step in understanding relevant privacy and security issues at a high level. Protecting Privacy in Connected Learning Toolkit is a more in depth, step-by-step guide to navigating the complexity of FERPA, COPPA and related privacy issues. Of course, considering the highly technical nature of privacy laws and policies, school leaders should always seek advice of legal counsel regarding such issues.

Prior versions of this Toolkit were created under a CoSN advisory board of school district and industry leaders, co-chaired by Bob Moore, Chief Technology Officer, Dallas Independent School District and Jim Siegl, Technical Architect, Fairfax County Public Schools.

Special thanks to those who took part in the development of the original Toolkit:

Rich Bagin, APR, Executive Director, National School Public Relations Association

David Bein, SFO, Assistant Superintendent of Business Services, East Maine School District 63

Shirley Broz, Retired, Former Director of Technology, Rockwood School District, Murrieta, CA

Robert L. Clayton, Counsel, Gonzalez Saggio & Harlan LLP

Linda Erdos, Assistant Superintendent, Arlington Public Schools, VA

Cameron Evans, National and Chief Technology Officer U.S. Education, Microsoft

Bill Kilcullen, Retired, Former Solution Regional Director, Microsoft

Bill Flaherty, Retired, Former Director of Technology, Glen Allen, VA

Claire Hertz, Chief Financial Officer, Beaverton School District, Beaverton, OR

Mara Ludmer, Student Attorney at the Cyberlaw Clinic, Harvard Law School

Evelyn McCormack, Director of Communications, Southern Westchester BOCES, NY

John D. Musso, CAE, Executive Director, Association of School Business Officials International Steve Mutkoski, Regional Director, Interoperability and Innovation, Microsoft

Kevin F. Supple, Chief Financial Officer, Francis Howell School District, MO

Dalia Topelson, Clinical Instructor and Lecturer on Law, Cyberlaw Clinic and Harvard Law School

Sonja H. Trainor, Director, Council of School Attorneys, National School Boards Association

Julie Zwahr, Director, Communications/Partnerships, Little Elm Independent School District, TX

CoSN would also like to thank the following for their support in preparing the inaugural Privacy Toolkit and the initial updates to the work:

Collaborating Organizations

- The Cyberlaw Clinic at Harvard Law School http://cyberlawclinic.berkman.harvard.edu/
- Berkman Klein Center for Internet & Society at Harvard University http://cyber.law.harvard.edu/
- Supporting Organizations
- Microsoft Education
- National School Boards Association Council of School Attorneys

FOR MORE INFORMATION, please contact: **Linnette J. Attai** | Project Director, CoSN's Protecting Privacy in Connected Learning Initiative and Trusted Learning Environment Program and President, PlayWell, LLC | **lattai@cosn.org**