



Protecting Privacy in Connected Learning

A CoSN Leadership Initiative

Protecting Privacy in Connected Learning Toolkit

Version 2, September 2014

Considerations When Choosing an Online Service Provider for your School System

Includes key information on FERPA (Family Education Rights and Privacy Act) and COPPA (Children's Online Privacy Protection Act)

plus...

- New sections on HIPAA (Health Insurance Portability & Accountability Act) and PPRA (Protecting Pupil Rights Amendment)
- Ten Steps Every District Should Take Today
- Infographic on Privacy Practices to Share with Parents/Guardians



In Partnership with Harvard Law School's Cyberlaw Clinic at the
Berkman Center for Internet & Society.



ACKNOWLEDGEMENTS

CoSN (the Consortium for School Networking) is the premier professional association for school system technology leaders. The mission of CoSN is to empower educational leaders to leverage technology to realize engaging learning environments.

Thank you to the Cyberlaw Clinic at Harvard Law School for helping CoSN in preparing this guide. **Harvard Law School's Cyberlaw Clinic**, which is based at the **Berkman Center for Internet and Society**, engages Harvard Law students in a wide range of real-world litigation, licensing, client counseling, advocacy, and legislative projects and cases, covering a broad spectrum of Internet, new technology, and intellectual property legal issues. Clients include individuals, small startups, nonprofit organizations, internal Berkman Center projects, groups of law professors, and government entities.

Endorsed by **The Association of School Business Officials International**.

Special Thanks to the **National School Public Relations Association** for partnering on the infographic on privacy practices.



CoSN

1025 Vermont Avenue NW, Suite 1010
Washington, DC 20005-3599
(202) 861-2676
www.cosn.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.

Protecting Privacy in Connected Learning Toolkit

TABLE OF CONTENTS

About this Resource 4–5

Introduction 6

Statutory Definitions 7

Step 1: Determining Your School System’s Needs 8

Step 2: Evaluating and Contracting with Online Service Providers..... 9

Step 3: Obtaining Parental Notification and Consent 10

Attachment #1: Defining Education Records 11

Attachment #2: Understanding Metadata and De-identification 12

Attachment #3: Security Questions to Ask of An Online Service Provider..... 13–14

Attachment #4: Suggested Contract Terms 15–17

Attachment #5: Unpacking “Click-Wrap” Software 18

Attachment #6: School Officials Exception 19

Attachment #7: Directory Information Exception 20

Attachment #8: HIPAA (Health Insurance Portability & Accountability Act) At-a-Glance . . . 21–22

Attachment #9: PPRA (Protecting Pupil Rights Amendment) At-a-Glance..... 23–24

Attachment #10: Ten Steps Every District Should Take Today..... 25

Attachment #11: Infographic..... 26–28

Useful Links 29–30

Special Thanks..... 31

VER. 2.0 UPDATES | SEPTEMBER 2014

Suggested Contract Terms—*Updated* Attachment 4 (pg. 15–17)

HIPAA— Attachment 8 (pg. 21)

PPRA— Attachment 9 (pg. 23)

Ten Steps Every District Should Take Today— Attachment 10 (pg. 25)

Infographic on Privacy Practices to Share with Parents/Guardians— Attachment 11 (pg. 26)

ABOUT THIS RESOURCE

It would be difficult to name an issue in recent years that has caused as much discussion and activity as protecting the privacy of students and their data. While much of the discussion is about compliance with Federal laws such as FERPA (Family Education Rights and Privacy Act) and COPPA (Children’s Online Privacy Protection Act), most agree that mere compliance is the minimum effort required by school systems and that concern for and protection of student privacy should become part of the fabric of education decision making, not just a compliance box to check.

When FERPA was enacted in 1974 no one could have imagined the implications for privacy in a world dominated by the Internet, cloud services, online learning and mobile apps. Even since COPPA went into effect in the year 2000, the world of education technology has changed radically. School System leaders wanted to act in the best interest of the students and families they serve, but applying laws that could not have foreseen profound technological advances is difficult at best. Coupled with the growing realization of the value of data for both educational and commercial purposes, school leaders can sometimes find themselves at odds with the very service providers they have come to depend on for valuable educational tools.

The value of technology tools and services in education has become undeniable. At the same time, the need to protect the privacy of students and their data is equally undeniable. School Systems have made much progress in recent years in using technology to personalize learning and create better learning opportunities for students. Educators and policymakers have also begun to realize the promise of using student data to make informed decisions, ranging from classroom instructional practices to investment in education programs. It is critical that leaders in education, industry and policy find ways to ensure student privacy, while continuing to encourage innovative uses of technology and student data.

Federal agencies are working hard to provide useful and clarifying information about privacy laws. Some states are seeking to enact their own student privacy legislation. Any number of organizations are working to release information that will help their own constituents understand their privacy obligations. School System leaders, particularly those leading school technology efforts, need information and guidance intended specifically for them and developed by those with a deep understanding of education technology leaders.

Since 1992 CoSN (Consortium for School Networking) 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.

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.

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.

Because navigating through privacy issues and compliance with FERPA and COPPA can quickly become confusing for school system leaders, the toolkit is organized in the form of a decision tree, or flowchart. FERPA and COPPA compliance issues are addressed, as are smart, suggested practices that reach beyond compliance.

Embedded in the toolkit's decision tree are definitions, checklists, examples and key questions to ask along the way. A significant amount of supporting information is also provided. For example, the toolkit offers a detailed definition 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 increasing use of Click-Wrap Agreements, common to so many popular, free online tools and services. A set of helpful Internet links to privacy-related resources is also included.

With the release of the original toolkit in March 2014, we promised that the CoSN Protecting Privacy in Connected Learning Toolkit would evolve just as the understanding of privacy laws and education technology evolves. In this version 2, released in September 2014, we have added four important components; "at-a-glance" briefs on the PPRA (Protecting Pupil Rights Amendment and HIPAA (Health Insurance Portability & Accountability Act), a document detailing steps every school district should be taking regarding privacy, and an infographic on privacy practices to share with parents/guardians. In addition, we have updated Attachment 4 on Suggested Contract Terms. Make sure you have downloaded the most recent version of the toolkit, as further updates and additions are planned.

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.



Protecting Privacy in Connected Learning

A CoSN Leadership Initiative

Protecting Privacy in Connected Learning Toolkit

INTRODUCTION

The purpose of this document is to help **School Systems** navigate some of the privacy issues that can arise when selecting and using an **online service provider**. The original version of this document focused on some of the obligations School Systems need to comply with under the Family Education Rights and Privacy Act (FERPA) and the Children's Online Privacy Protection Act (COPPA), as well as suggested industry practices to protect the privacy of student information. This most recent version, released in September 2014, also includes at-a-glance summaries of the two other Federal privacy laws applicable to K12 School Systems, the PPRA (Protecting Pupil Rights Amendment) and HIPAA (Health Insurance Portability & Accountability Act). It should be noted that this document only covers some of the obligations, and School Systems may be subject to other federal and state privacy laws that are not covered by this document. Further, 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 Systems.

It is also important to remember that protecting the security of student information will likely require your School System to look beyond the letter of the law. In the words of the U.S. Department of Education's (ED) Chief Privacy Officer, Kathleen Styles, "FERPA is the floor. The ceiling is something very different. Achieving compliance with FERPA is not the end of the story." For that reason, this document includes industry suggested practices.

For a more detailed description of student privacy rights please see the U.S. Department of Education's [Protecting Student Privacy While Using Online Education Services: Requirements and Best Practices](#) and the Berkman Center at Harvard University's [FERPA/COPPA Guide](#).

For purposes of this document, the terms below are defined as follows:

Online Service Provider:

a provider that offers technological tools such as calendars, word processing, online quizzes, and interactive games that are available for access through the Internet, from a computer, or mobile devices.

School System(s):

for the purposes of this document, School System(s) refers to schools, districts, local education agencies.

Flow Chart Key



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.

STATUTORY DEFINITIONS

This section of the document provides you with the definitions of key terms, as defined by the relevant statute. You should note that FERPA and COPPA define similar terms differently, so please use this definition section in partnership with the flowchart to help you understand how these laws might apply to your School System.

COPPA Definitions

Personal Information:

Name, home address, email address, telephone number, social security number, photo, video, audio files containing child's voice, geo-location information, persistent identifier that can be used to recognize use over time and across different websites, and any other information that permits physical or online contact of a specific individual.

FERPA Definitions

Personally Identifiable Information (PII):

PII is the name of a student or family member, address, personal identifiers (e.g. social security number), indirect identifiers (e.g. date of birth), and other information whereby a "reasonable person in the school community" could identify the student.

Education Records:

Materials that are "maintained by an educational agency or institution or by a person acting for such an agency or institution," and contain information directly related to a student.

For a list of what is not considered an education record, [See Attachment #1.](#)

Directory Information:

Name, address, telephone listing, 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 sports and other activities. Does not include social security number.

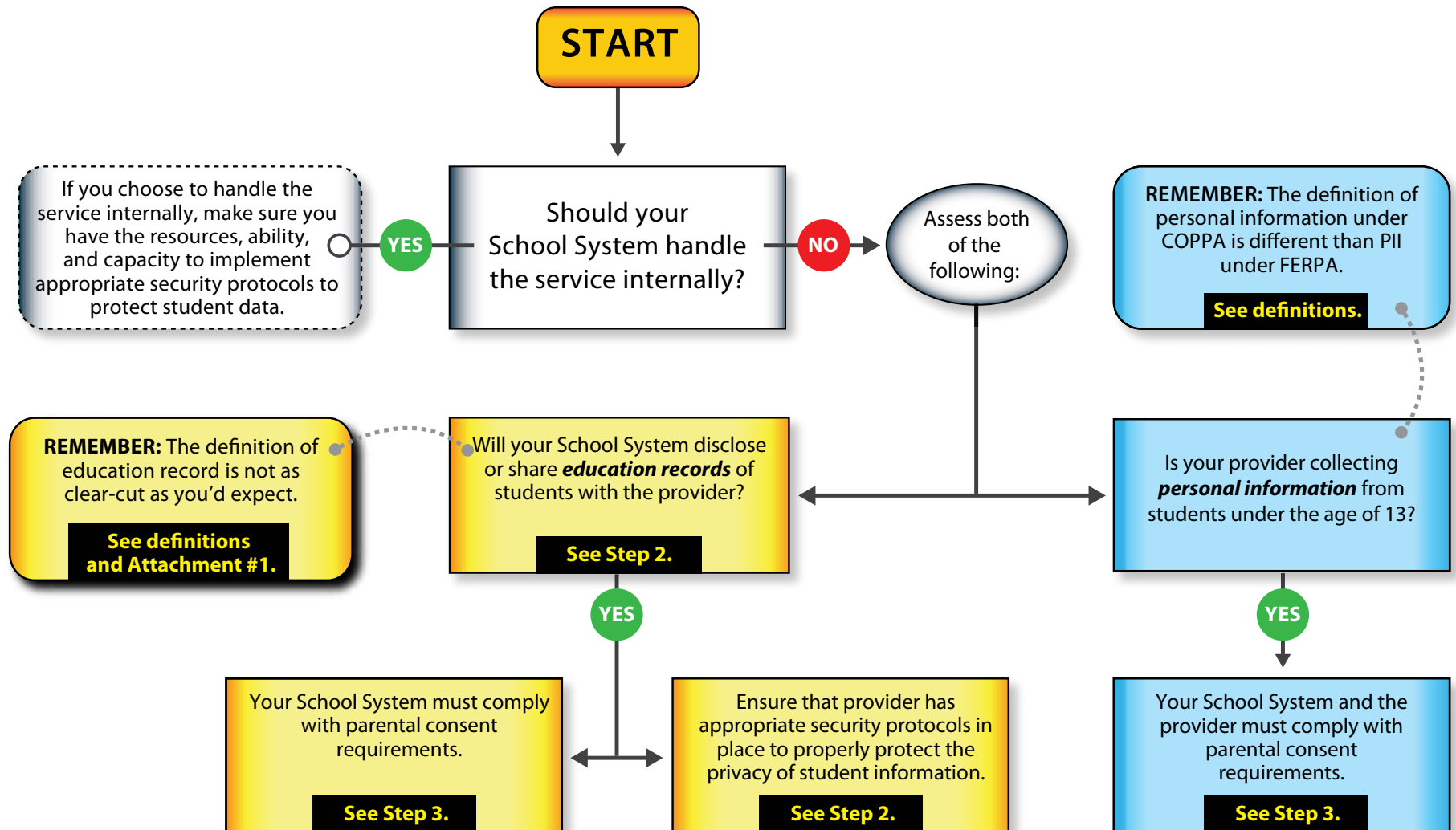
De-Identified Data:

The School System has removed all personally identifiable information and there is a reasonable determination that the student is not identifiable.

[See Attachment #2.](#)

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.

STEP 1: DETERMINING YOUR SCHOOL SYSTEM'S NEEDS

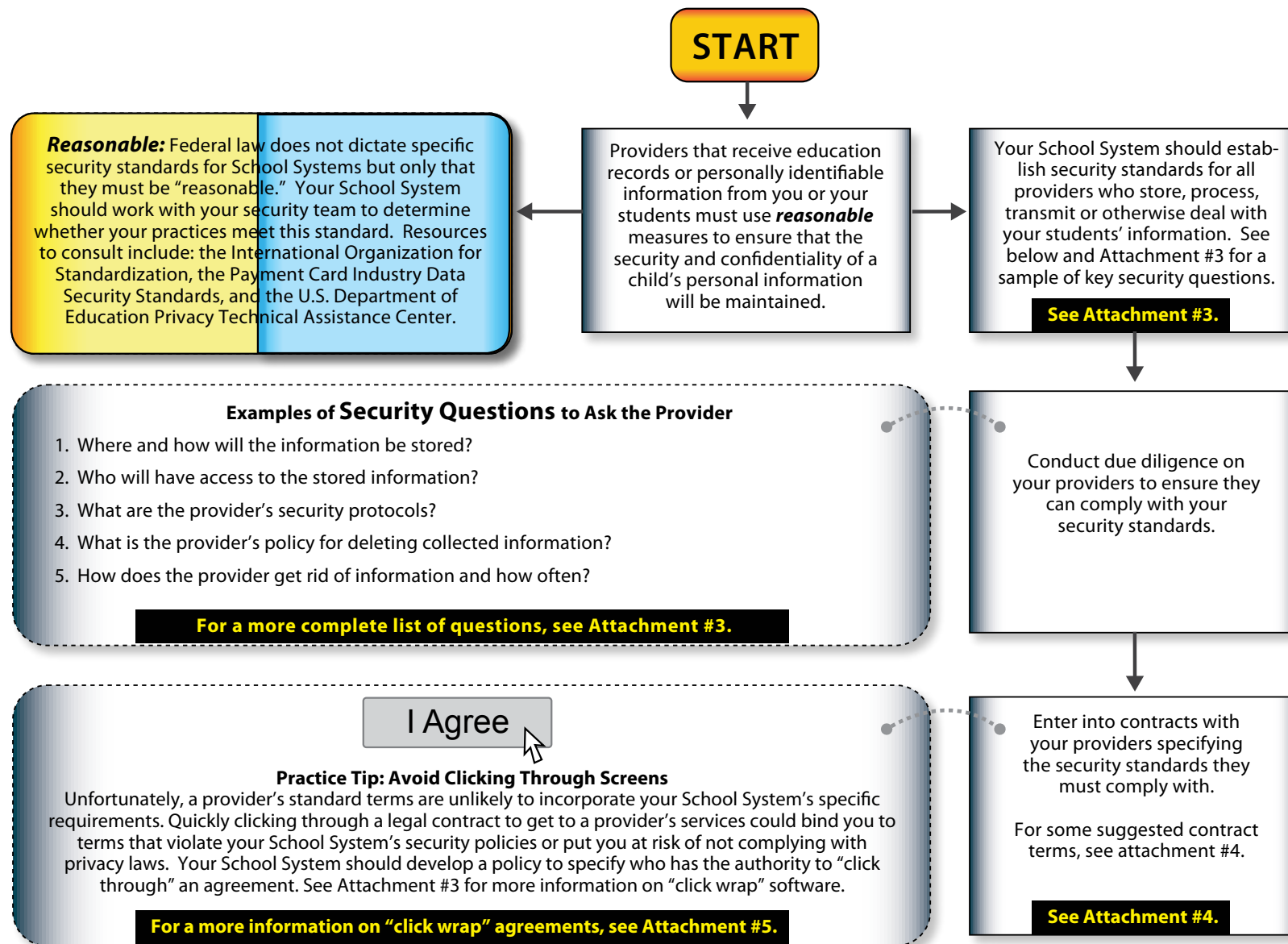


Flow Chart Key



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.

STEP 2: EVALUATING AND CONTRACTING WITH ONLINE SERVICE PROVIDERS

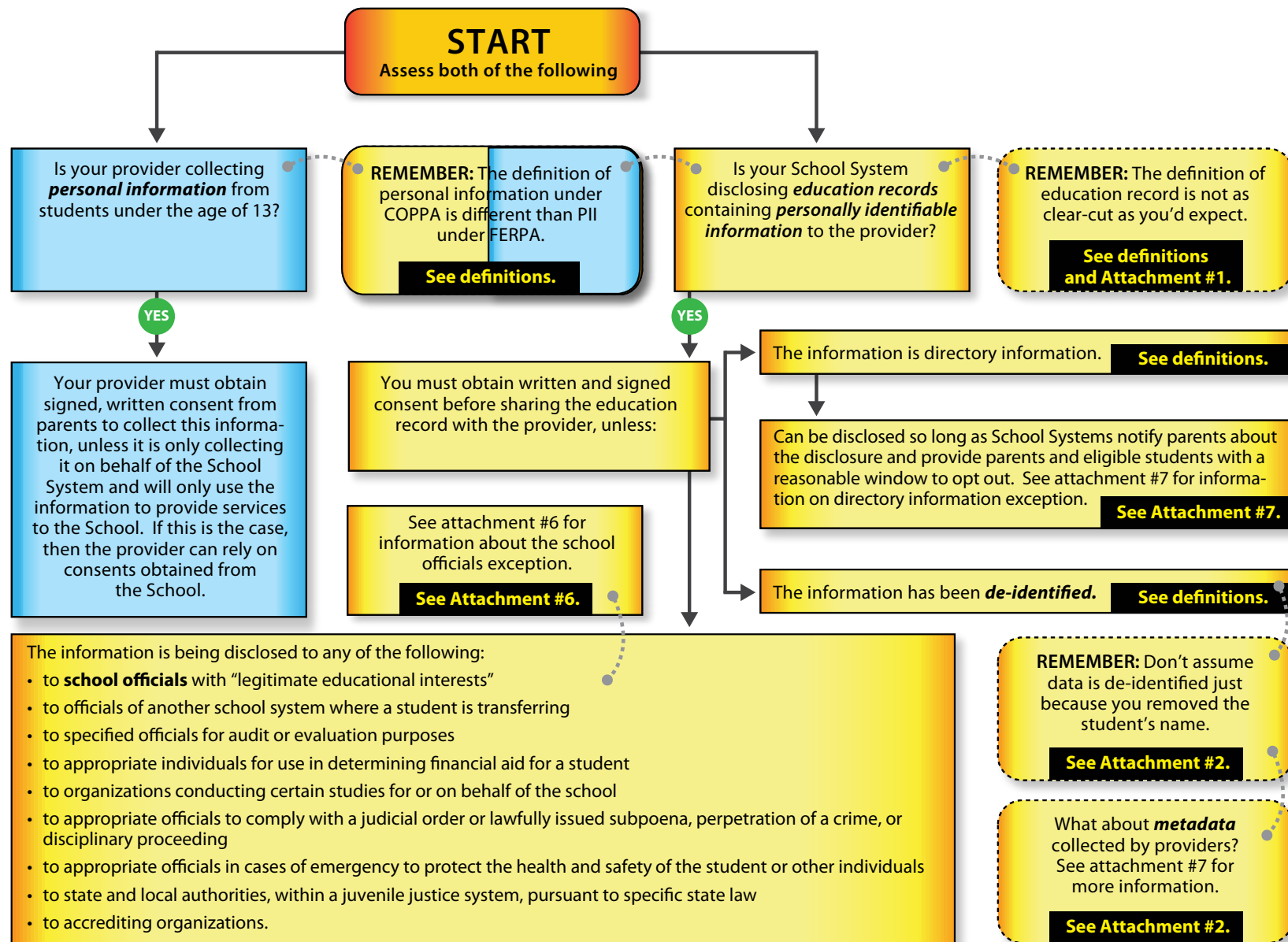


Flow Chart Key



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.

STEP 3: PROVIDING NOTIFICATION AND OBTAINING PARENTAL CONSENT



Flow Chart Key



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.

#1 Defining Education Records

Just what is or is not an education record is not as clear-cut as you might expect, particularly as we consider how school systems generate and collect records using new types of technologies. To that end, you should ***assess whether the records or information being generated, stored or processed by a provider qualify as an education record with your School System’s legal counsel*** before proceeding.

As explained in the flowchart, ***education records*** are materials “maintained by an educational agency or institution or by a person acting for such an agency or institution,” and contain information directly related to a student. 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 shared with anyone besides a temporary substitute
- Records maintained by an educational agency’s law enforcement unit
- Employee records made in the normal course of business and that pertain only to the individual’s employment
- Records of a student over the age of 18 or who is attending postsecondary education made by professionals such as a physician or psychiatrist for treatment of the student; this information can only be disclosed to those who provide the treatment
- Records that an educational agency made or received after the student stopped attending the institution; these records cannot directly relate to the student’s attendance
- Grades on peer-reviewed papers before they are collected and recorded by a teacher

For more information, see ED’s [Protecting Student Privacy While Using Online Education Services: Requirements and Best Practices](#) and the Berkman Center at Harvard University’s [FERPA/COPPA Guide](#).

#2 Understanding Metadata and De-identification

As acknowledged by the ED, many online educational services collect “large [amounts] of contextual or transactional data as part of their operations, often referred to as ‘metadata.’” For example, the ED explains that information on how many times a student tries before succeeding at a task, or the amount of time a student’s mouse lingers over an answer before clicking on it, qualifies as metadata. While metadata can provide extremely valuable information about a student, it can also be used to identify a student. To that end, School Systems should treat metadata in the same way as all other types of personally identifiable information. That said, once all information linking metadata to a student has been removed, the ED has stated that it qualifies as de-identified data, and accordingly both School Systems and providers can do what they wish with that data.

The “de-identification” of data, including metadata, raises some highly challenging issues and you will probably want to consult your School’s counsel, as well as an expert in data issues before you undertake to de-identify data or allow a service provider to do so. Importantly, FERPA’s definition of personally identifiable information includes a catch all that references “information, that alone or in combination, is linked or linkable to a specific student” and there is no statutorily approved method for de-identifying FERPA protected information. Because de-identification is more of an art than a science, you will want to engage competent experts to review any plans you have or a provider has to de-identify any FERPA protected data. De-identification of data is a tricky process. 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.” If your School System remains concerned about how providers use metadata (including de-identified data), the ED suggests you negotiate stricter contractual terms with the provider about how metadata can be collected and used.

For more information, see ED’s [Protecting Student Privacy While Using Online Education Services: Requirements and Best Practices](#).

#3 Security Questions to Ask of An Online Service Provider

It is important to understand your provider's security practices to ensure that data shared with and collected by the provider remain private and protected. You should work with your School System's security point of contact to determine whether the security practices of the provider comply both with School System policies and applicable laws. While neither FERPA nor COPPA prescribes specific security standards, school systems should 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. A service level agreement (SLA) should include as many of these considerations as possible.

1. Data Collection

- What data does the provider collect?
- What, if any, data is collected by 3rd parties (e.g., via cookies, plug-ins, ad networks, web beacons etc.)?

2. Network Operations Center Management and Security

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

3. 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, all data) and what encryption method is used?
- 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?
 - FERPA requires that records for a school be maintained separately, and not be mingled with data from other school systems or users.
- Are the physical server(s) in a secured, locked and monitored environment to prevent unauthorized entry and/or theft?
- How does the provider protect data in transit? e.g. SSL, hashing?
- 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, applications and customer data?
 - Does the provider subcontract any functions, such as analytics?
 - What is the provider's process for authenticating callers and resetting access controls, as well as establishing and deleting accounts?
- If student or other sensitive data is transferred/uploaded to the provider, are all uploads via SFTP or HTTPS?

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.

4. Data and Metadata Retention

- How does the provider assure the proper management and disposal of data?
–The provider should only keep data as long as necessary to perform the services to the School.
- How will the provider delete data?
–Is data deleted on a specific schedule or only on termination of contract? Can your School request that information be deleted? What is the protocol for such a request?
- You should be able to request a copy of the information maintained by the provider at any time.
- All data disclosed to the provider or collected by the provider must be disposed of by reasonable means to protect against unauthorized access or use.
- Upon termination of the contract, the provider should return all records or data and properly delete any copies still in its possession.

5. Development and Change Management Process

- Does the provider follow standardized and documented procedures for coding, configuration management, patch installation, and change management for all servers involved in delivery of contracted services?
- Are practices regularly audited?
- Does the provider notify the School System about any changes that will affect the security, storage, usage, or disposal of any information received or collected directly from the School?

6. 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?

7. Audits and Standards

- Does the provider provide the School System the ability to audit the security and privacy of 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), the Payment Card Industry Data Security Standards (PCI DSS)?

8. Test and Development Environments

- Will "live" student data be used in non-production (e.g. test or development, training) environment?
- Are these environments secure to the same standard as production data?

9. Data Breach, Incident Investigation and Response

- What happens if your online service provider has a data breach?
- Do you have the ability to perform security incident investigations or e-discovery? If not, will the provider assist you? For example, does the provider log end user, administrative and maintenance activity and are these logs available to the School System for incident investigation?

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.

#4 Suggested Contract Terms

After your School System chooses an online service provider, it is important to draft a contract that specifies how the provider will comply with your School System's security requirements. Drafting 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 including.

The contract should specify the services to be provided and the provider's obligations, including the following:

1. **Contract Scope.** Identify all elements that comprise the agreement and what order of precedence is followed in the event of a contradiction in terms. Identify any contract terms that are incorporated by reference (e.g. URL).
2. **Purpose.** If you have determined that the provider qualifies as a "school official" under FERPA and you will use the school officials exception as the vehicle for disclosing FERPA protected information to a provider, specify: (i) that the provider is considered a school official, (ii) the legitimate educational interest that the provider is fulfilling, (iii) the nature of the data collected, and (iv) the purpose for which any FERPA protected information is being disclosed.
3. **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 and ensure that you bind the provider to those uses and restrictions. At a minimum, you should address the following:
 - Specify that the provider should only be permitted to use any information stored, processed, or collected as necessary to perform the services for the School System. Include a specific restriction on the use of student information by the provider for advertising or marketing purposes, or the sale or disclosure of student information by providers.
 - Specify any metadata the provider will collect (e.g. logs, cookies, web beacons, etc.).
 - Specify any data and metadata any 3rd party will collect (e.g. analytics, etc.) as a function of the use of the provider's service.
 - Specify that the provider should be restricted from accessing, collecting, storing, processing or using any school records, and student or parent information, for any reason other than as necessary to provide the contracted services to your School.
 - Specify when and how the provider may disclose information it maintains to other third parties. Under FERPA, providers may not disclose education records provided by your School System to third parties unless specified in your contract.
 - Specify whether the School System and/or parents (or eligible students) will be permitted to access the data (and if so, which data) and explain the process for obtaining access. Consider if the contract needs to specify whose responsibility it is (the provider or the School System) to obtain parental consent and facilitate parent's request to access student educational records.

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.

- Specify that data collected belongs to the School System (and/or its users) and that the provider acquires no rights or licenses to use the data for purposes other than for the delivery of the service.
 - Specify that a provider must disclose if it will de-identify any of the FERPA protected data that it will have access to and if so, require that the provider supply details of its de-identification process. When appropriate, you may want to retain rights to approve such a process prior to the provider using or sharing de-identified data in ways that are beyond the purpose for which any FERPA protected information is disclosed.
- 4. Data Security.** Specify any security requirements that the provider must follow to the extent that it maintains, processes, or stores any information on behalf of the School System. At a minimum, the contract should address the following:
- The provider must securely maintain all records or data either received from the School System or collected directly from the school, teachers, students, or parents in accordance with the security standards designated by the School.
 - Information, content and other data collected and stored from and on behalf of the School System and the students should be stored and maintained separately from the information of any other customer, school, or user.
 - The provider should restrict access to your School System's information to only those individuals that need to access the data in order for the provider to perform the agreed-upon services.
 - The agreement should identify what happens if the provider has a data breach. The agreement should identify the provider's responsibilities including the School System's point of contact, required notification time, and any obligations for end user notification and mitigation.
 - You should have the right to audit the security and privacy of your School System's or students' records or data.
 - Require the provider to notify you in writing about any changes that will affect the availability, security, storage, usage or disposal of any information.
- 5. Data Retention and Disposal.** Assure the proper management and disposal of data or information pertaining to the School or its students. All 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.
- 6. Bankruptcy or Acquisition.** Specify what happens to the data if the provider goes out of business or is acquired by another firm. Is there a source code or data escrow provision?
- 7. Service Levels and Support.**
- Specify the service levels the provider must meet and any credits you receive for any failure by the provider to meet these service levels.
 - Require the provider to supply the School with all the technical assistance you may need to use the services.

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.

- 8. 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 in light of your School's state laws.
- 9. Modification, Duration, and Termination Provisions.** Establish how long the agreement will be in force, what the procedures will be for modifying the terms of the agreement (mutual written consent to any changes is a best practice), and 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 records or data and properly delete any copies still in its possession, including archives and/or backups.
- 10. Liability.** The provider should be liable for the activities of its staff and subcontractors.
- The provider should generally have an obligation to comply with all applicable laws, including privacy laws.
 - If the provider will be collecting data from children under the age of 13, the provider should comply with COPPA.
 - The provider should be liable for any breaches in security or unauthorized third party access arising out of the provider's breach of its contract obligations.
 - The provider should be liable to the School System for any claims or damages that arise as a result of the provider's failure to comply with its obligations as a Cloud Service Provider under COPPA, FERPA, or other applicable laws.
 - Limits of liability should be consistent with market-tested commercial practices and should appropriately allocate risk between the Vendor as a Cloud Service Provider and the Customer as the owner of its Data.
 - The School System may wish to identify through negotiation specific categories of direct damages that would be excluded from traditional definitions of consequential damages.

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.

#5 Unpacking “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) without reading it to gain access to technological tools, her actions can bind the School System to terms that don’t align with security protocols and policies, and can put the School System at legal risk if the provider’s practices fail to comply with privacy laws that apply. It is important to develop a procedure for assessing providers’ contracts to ensure that the provider will comply with your School System’s security policies, and to provide the School System with some contractual remedies if the provider fails to either meet these standards or comply with applicable law.

When reviewing a “click-wrap” contract, you should not only look for a provider’s obligations to maintain the privacy of your students’ data, but you should also be on the lookout for provisions that give the provider the right to amend the contract without notifying you or gaining your consent. The ED points out that these amendment provisions are particularly problematic under the school official exception of FERPA where School Systems must maintain **direct control** over the data. The ED also recommends always printing the Terms of Service agreement of a “click-wrap” provider. ED even recommends “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 it may not be practical, or even possible, for your School System to negotiate with every provider, making it more likely that someone at your School System may want to onboard a technology under a “click-wrap” agreement, your school should think about ways to streamline the contracting process so that selecting an online service provider does not impact obtaining rich tools that could benefit the students in the classroom. A number of options are available to your School System to address this problem. First, you can work with legal counsel to establish a list of preferred providers for your School System. Another option is to have legal counsel create a rider containing the School System’s minimum requirements and obligations that teachers or other employees can give to providers to sign before utilizing their services. Finally, consider establishing a policy that designates which employees in your School System are authorized to click through provider agreements, then provide adequate information to these individuals so that they can make informed decisions in regard to contracting with providers.

For more information, see ED’s [Protecting Student Privacy While Using Online Education Services: Requirements and Best Practices](#).

#6 School Officials Exception

According to the ED, a provider must meet the following requirements in order to qualify as a “school official”:

1. The provider must “[perform] an institutional service or function for which the School System would otherwise use its own employees.”
2. The School System must determine that the provider has a **legitimate educational interest** in the education records. Any determination must be consistent with the School System’s policies and annual notice to parents defining a legitimate educational interest.
3. The provider must be “under the **direct control** of the School System with regard to the use and maintenance of education records,” meaning that the School System can control how the provider uses, processes and collects this information. As noted by the ED, this control can usually be established through a contract between the parties, so long as the agreement contains “all of the necessary legal provisions governing access, use and protection of the data” to ensure that the School System can contractually control the behavior of the provider.
4. Except for metadata which has been de-identified (**see Flowchart Step 3 and #7 Metadata**), the provider may only use the education records for the purposes for which the disclosure was made,” and for no other purpose. Further, the provider may not re-disclose the education records to any other person or party without further authorization from the School.

The U.S. Department of Education’s newly issued guidance includes some important discussion and examples related to the fourth requirement above that you should review carefully. The guidance highlights that providers may want to use information for purposes other than for which it was received, such as “marketing new products or services to the student, targeting individual students with directed advertisements, or selling the information to a third party.” The ED guidance, and included examples (such as the example provided below), make clear that such uses are not permitted under FERPA.

For more information, see ED’s [Protecting Student Privacy While Using Online Education Services: Requirements and Best Practices](#).

AN EXAMPLE OF THE SCHOOL OFFICIAL EXEMPTION

“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.”

Source: ED’s [Protecting Student Privacy While Using Online Education Services: Requirements and Best Practices](#).

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.

#7 Directory Information Exception

The flowchart lists the type of information that qualifies as “directory information,” such as student name, address, telephone listing, email address, etc. As noted in the flowchart, a School System can disclose directory information without consent, so long as the School System notifies the parents and students of the data to be disclosed and provides parents or eligible students with a reasonable amount of time to opt out of the disclosure. As noted by the ED, many School Systems provide a list of data that will be disclosed annually to parents and students, who can then opt out of disclosure.

The ED points out that while sharing information with online service provider under this exception may appear to be a good option for School Systems, it has two major drawbacks: First, only directory information flagged in the public notice may be disclosed using this exception. Second, the fact that parents and students may, and often do, “opt out” of disclosing their information can create an imbalance in the classroom environment if some students have opted out of disclosure while others have not. The ED suggests that the school officials exception (**#6 School Officials Exception**) is likely a better option for School Systems to use to share information with an online service provider.

For more information, see ED’s [Protecting Student Privacy While Using Online Education Services: Requirements and Best Practices](#).

#8 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 (HITECH¹), part of the American Recovery and Reinvestment Act, incorporated new provisions into HIPAA’s Privacy² and Security³ Rules. HITECH established that the Department of Health and Human Services (HHS) would issue guidance regarding technological methods for protecting health information. In addition, HITECH extended HIPAA enforcement to service providers or “business associates” who help manage and transmit health information on behalf of a “covered entity.”

It should be noted that while HIPAA is important to understand, its application in K12 schools is limited. Most student records, including health records, are education records or treatment records, which are covered by FERPA. However, generally, School Systems are subject to HIPAA if they are providing health services and electronically transmit “health information” for any of the following purposes:

- To process health care claims or equivalent encounter information
- To process health care payments and provide remittance advice
- To coordinate benefits
- To check or process health care claim status
- To enroll or process the disenrollment of individuals in a health plan
- To determine eligibility for a health plan
- To process health plan premium payments
- To certify and authorize referrals
- To process the first report of injury
- To manage and process health claims attachments
- To 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. Accordingly, in addition to the contractual provisions covered in [Attachment #4 \(Suggested Contract Terms\)](#), you should include an obligation to comply with HIPAA, and also have your online service provider execute a *Business Associate Agreement*⁴.

It should be noted that student health information maintained by most K-12 School Systems is usually not subject to HIPAA. As noted in the U.S. Department of Health and Human Services and the U.S. Department of Education’s *Joint Guidance⁵ 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

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.

Guidance”), “At the elementary or secondary level, a student’s health records, including immunization records, ... as well as records maintained by a school nurse, are education records subject to FERPA.” This is because these records are generally directly related to the student, and are maintained by the school for its purposes, rather than to process the transactions set forth above. That said, if your School System hires a health care provider to treat kids, for instance, to provide broader healthcare to an underserved population, your School System may be subject to HIPAA. Likewise, HIPAA may apply to health information related to your School System’s staff, teachers and other employees.

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 could provide good guidance on how to ensure you are securing your students’ information more broadly.

1. You can access more information on the HITECH Act at <http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitech enforcementifr.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 a sample Business Associates Agreement, visit: <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html>
5. 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 \(2008\)](#).

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.

#9 PPRA (Protecting Pupil Rights Amendment) At-a-Glance

The Protection of Pupil Rights Amendment (the “PPRA”) applies, with some minor exceptions, to any program that receives funding from the Department of Education. Generally, the PPRA requires School Systems to obtain consent from parents or students over the age of 18 before administering a survey, analysis or evaluation that requires students to share certain types of sensitive information, such as:

- Political affiliations of the student or the student’s parent
- Mental and psychological problems of the student or the student’s parent
- Sex behaviors and attitudes
- Illegal, anti-social, self-incriminating, or demeaning behavior
- Critical appraisals of individuals that have a close family relationship with the student
- Legally privileged information, 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)

The law also requires School Systems to provide parents and eligible students with access to instructional materials that are used in connection with the survey, analysis or evaluation.

Requirements applying to K-12 School Systems Only

Development of Policies

In addition to the requirements described above, which apply to all educational institutions receiving funding from the Department of Education, K-12 School Systems are required to do the following:

- Develop policies, in consultation with parents, addressing:
 - How the School System plans to protect the privacy of the sensitive information described above that is collected by the School System, whether or not that information is collected as part of a survey, analysis or evaluation;
 - How parents and eligible students can inspect surveys before they are administered, as well as instructional materials used as part of the educational curriculum;
 - The administration of physical exams or screenings that the School System may administer to students;
 - How the school plans to collect, disclose and protect personal information collected from students for marketing purposes or for purposes of selling that information; and
 - The right of parents to inspect any instrument used to collect information to sell or for marketing purposes before it is used with the students, including the procedures to provide parents and eligible students with that access.

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.

The PPRA does allow School Systems to collect personal information for marketing purposes or to sell the information without developing a policy, if, and only if, the information will only be used to develop, evaluate, or provide educational products or services that will be used by or for students or educational institutions generally. For example, you do not need to develop a policy if you plan to collect personal information from your students to sell to universities for recruitment purposes or to market low-cost literary products to students.

Despite this exception, as a best practice, you should create policies on how you plan to collect information for sale or marketing purposes, regardless of why you or your service provider are collecting this information. This will help ensure that parents understand how their children's information is being used, and will help avoid taking parents by surprise, even if the activity you are engaged in may be legal.

Parental Notification and Opt-Out

In addition to requiring School Systems to develop certain policies, the PPRA also imposes obligations on K-12 School Systems that participate in any of the following activities:

- The collection of Personal Information from students to use for marketing or to sell to another party
- Any survey that asks students to provide Sensitive Information
- Any invasive, nonemergency physical examination that is required as a condition of a student's school attendance

If you participate in any of these activities, you must:

- Notify parents and students 18 and older of policies surrounding these activities
- Notify parents and students 18 and older of times and dates when you plan to perform any of these activities
- Provide parents or students 18 and older the opportunity to opt-out of these activities

Applying the PPRA in the Online Context

The PPRA applies, regardless of whether or not you use an Online Service Provider to administer a survey, or to store or collect the information that is covered by the statute. To that end, similar to the guidance provided regarding FERPA, the Department of Education suggests that you implement contractual limitations as to how and when your Online Service Provider can use and disclose data collected from students. This is particularly important considering the restrictions the PPRA has related to the use of student information for marketing purposes and the sale of this information. For more information on what terms you should include in a contract, see [Attachment #4 \(Suggested Contract Terms\)](#).

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

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.

#10 Ten Steps Every District Should Take Today

With so much uncertainty about what districts can or should be doing to help ensure the privacy of student data, it would 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. This is a “divide and conquer” issue, but someone needs to be in-charge.
2. **Seek Legal Counsel**—Make sure that the legal counsel 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. **Know the Laws**—Many organizations have and will be publishing privacy guidance for schools, such as the toolkit CoSN toolkit available at <http://www.cosn.org/privacy>. The US Department of Education’s Privacy Technical Assistance Center is a must-know resource at <http://ptac.ed.gov/>.
4. **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.
5. **Implement Workable Processes**—There must processes for selecting instructional apps and online services. No one wants to slow innovation, but ensuring privacy requires some planning and adherence to processes. Once enacted, the processes should be reviewed regularly to ensure that they are workable and that they reflect current interpretations of privacy laws and policies.
6. **Leverage Procurement**—Every bid or contract has 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. Unfortunately, many online services are offered via “click-wrap” agreements that are “take it or leave it.” You may have to look for alternatives solutions if the privacy provisions of those services do not align with your expectations.
7. **Provide Training**—Staff need training so they will know what to do or 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 the measures taken to protect student privacy.
9. **Make Security a Priority**—Privacy starts with security. Secure the device, the network and the data center. Toughen password policies. Have regular security audits conducted by a third party expert.
10. **Review and Adjust**—Interpretations of privacy laws are changing and new laws may be added. School policies and practices will need updating and adjusted so that they reflect legal requirements. Processes can become burdensome when that happens, some people may want to skirt the process.

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.

#11 Infographics

CoSN and the National School Public Relations Association (NSPRA) teamed to produce two infographics (see pages 27 & 28) that empower school leaders to discuss the critical issue of student privacy. Parents and community members are justifiably concerned and confused about privacy in schools. How should you lead a discussion with these stakeholders about privacy? The infographic breaks down what's important and demystifies the issues.

Available in English and English/Spanish, the customizable infographics answer key questions such as: What data is collected and why? How does education data support student success and school improvement? How is education data protected?

For customizable version of the infographic, please visit www.CoSN.org/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.



Our Commitment to You: **CLEAR PRIVACY PRACTICES**

Parents and guardians want assurances that personal information and data about their children are secure and protected by our school system. These questions are rising as we use the Internet, mobile apps, cloud computing, online learning and new technologies to deliver exciting new education services.

At our school, we strive to be clear about what data we collect, how data support your child's education and the safeguards in place to protect that data.

What Data do We Collect and Why?



School Operations

We collect data such as addresses and phone numbers, gender and age, as well as information to ensure student safety and accurate reporting to help run our school operations efficiently.



Measuring Progress and Participation of our Students

We collect data such as attendance, grades and participation in school-sponsored extra-curricular activities to enable students to succeed.

Improving the Education Program

We collect results from local, state and national assessments to provide teachers, administrators and parents important information about student, program and school performance and improve the education programs we offer.



Striving to Meet the Needs of Students

We collect surveys and other feedback to improve teaching and learning and address other issues important to students and their families.



How Do Education Data Support Student Success and School Improvement?

data=success!

TEACHERS need data to understand when students are thriving and when they need more support in learning specific concepts.

PARENTS and guardians need access to their child's educational data to help them succeed.

STUDENTS need feedback on their progress so they can make good decisions about program choices and prepare for success.

SCHOOL OFFICIALS and community members need to understand school performance and know if scarce education resources are being allocated fairly and effectively.

How is Education Data Protected?

We follow federal and state education privacy laws and adhere to privacy and security policies.

» For example, the Family Education Rights & Privacy Act (FERPA) gives parents rights related to their children's education records and personally identifiable information. Additional information is available in our annual notice to parents of their rights under FERPA and from the U.S. Department of Education at <http://familypolicy.ed.gov/>.

When we use an online service provider to process or store data, they also must adhere to certain federal and state and privacy laws. We also expect them to use current security protocols and technology.

» Additionally, the federal Children's Online Privacy Protection Act (COPPA) prevents child-directed websites and apps from collecting certain personal information from anyone under 13 years of age without parental permission. Our school system may consent on behalf of parents in the education context when student information is collected for the school's exclusive use and benefit and for no other commercial purpose.

» Under FERPA, our vendors cannot use the education records we provide in any way that is not authorized by the school district. They cannot sell this data or allow others to access it except as we permit in accordance with federal and state education privacy laws.

Our Commitment

We are working to improve your children's education by ensuring it meets their unique needs. It would be very difficult to accomplish this goal without the ability to capture important information about your child's progress. Protecting personal information in secure and responsible ways is at the heart of our efforts to provide a richer and more dynamic learning experience for all students.

LEARN MORE about the rights of parents and guardians at dataqualitycampaign.org/pta or PTA.org/Parents or commonsensemedia.org

USEFUL LINKS

Collaborating Organizations

- The Cyberlaw Clinic at Harvard Law School <http://cyberlawclinic.berkman.harvard.edu/>
- Berkman Center for Internet & Society at Harvard University <http://cyber.law.harvard.edu/>

Supporting Organizations

- Microsoft Education <http://www.microsoft.com/education/ww/Pages/index.aspx>
- National School Boards Association Council of School Attorneys <http://www.nsba.org/SchoolLaw/COSA>
- Association of School Business Officials International <http://asbointl.org/>

Legislation

- *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. Resources include a data sharing agreement, data privacy and security governance checklists, security best practices, and a model notification of rights.
- *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>

Technology and Contracting

- CoSN Initiatives: Cyber Security for the Digital District <http://www.cosn.org/cybersecurity>
- CoSN Member Only Resources: available from 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
- K-12 Edtech Cloud Service Inventory http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2378570&rec=1&srcabs=2378568&alg=1&pos=1
- Security Guidance for Critical Areas of Focus in Cloud Computing V3.0, Cloud Security Alliance (CSA) <https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf>
- Privacy and Cloud Computing in Public Schools, Fordham University <http://law.fordham.edu/center-on-law-and-information-policy/30198.htm>

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.

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/>
- Common Sense Media Survey http://cdn2-d7.ec.commonsensemedia.org/sites/default/files/uploads/about_us/student_privacy_survey.pdf

Policy and Advocacy

- Student Privacy in the Cloud Computing Ecosystem: State of Play & Potential Paths Forward, Berkman Center for Internet & Society <http://cyber.law.harvard.edu/node/8638>
- Student Privacy and Cloud Computing at the District Level: Next Steps and Key Issues, Berkman Center for Internet & Society http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2378568
- Data Privacy and Schools: Outlining the Conversation (iKeepSafe.org)
<http://www.ikeepsafe.org/educators/schoolprivacy/>
- Digital Compliance and Student Privacy: A Roadmap for Schools (iKeepSafe.org)
<http://www.ikeepsafe.org/educators/digital-compliance-and-student-privacy-a-roadmap-for-schools/>
- EPIC Op-Ed: <http://www.washingtonpost.com/blogs/answer-sheet/wp/2014/03/06/why-a-student-privacy-bill-of-rights-is-desperately-needed/?print=1>

Training, Education and Communication

- Lesson Plans: What's The Big Deal About Internet Privacy? Common Sense Media
<http://www.commonsensemedia.org/educators/lesson/whats-big-deal-about-internet-privacy-6-8>
<https://www.commonsensemedia.org/educators/lesson/privacy-rules-3-5>
- What Every Parent Should Be Asking about Education Data and Privacy, Data Quality Campaign
<http://www.dataqualitycampaign.org/find-resources/what-every-parent-should-be-asking-about-education-data-and-privacy>
- Myth Busters: Getting the Facts Straight about Education Data, Data Quality Campaign
<http://www.dataqualitycampaign.org/files/Education%20Data%20Privacy%20Myth%20Busters.pdf>
- Data Privacy and Schools: Outlining the Conversation
<http://www.ikeepsafe.org/educators/schoolprivacy/>

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.

CoSN Privacy Educator Advisory Panel

Co-Chairs

Bob Moore, Founder	RJM Strategies LLC
Jim Siegl, Technical Architect	Fairfax County Public Schools
Sheryl Abshire, Chief Technology Officer	Calcasieu Parish Public Schools
Curt Cearley, Director	Fayette County Board of Education
Matt Cormier, Executive Director, Educational Technology	Jefferson County Public Schools (CO)
Vince Humes, Director of Technology and Solution Services	Northwest Tri-County Intermediate Unit #5
Tony Inglese, Chief Information Officer	Batavia Public Schools
Theresa Jay, Director of Technology	Thayer Academy
Greg Mortimer, Senior Director of Infrastructure and Development	Denver Public Schools
Chelsea Rock, Director of Technology	District of Columbia Public Schools
Melissa Tebbenkamp, Director of Instructional Technology	Raytown Quality Schools
Jean Tower, Director of Technology	Public Schools of Northborough & Southborough
Steve Young, Chief Technology Officer	Judson ISD

Special thanks to those who took part in the development of this 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, 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

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.