Protecting Privacy
in Connected Learning
A CoSN Leadership Initiative

Protecting Privacy in Connected Learning Toolkit

Version 1, March 2014

Considerations When Choosing an Online Service Provider for your School System

CoSN
LEADING EDUCATION INNOVATION

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

Sponsored by Microsoft

CoSN

LEADING EDUCATION INNOVATION

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.

Sponsored by Microsoft

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

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 want 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 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, but School System leaders and 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.

Because the interpretation of privacy laws is evolving, as well as privacy laws themselves and the technology services they seek to govern, the CoSN *Protecting Privacy in Connected Learning Toolkit* will also evolve. Working with even a wider array of partners, additional resources will be added to the toolkit throughout the year so that it stays relevant and provides increasing value to the school system technology leaders we serve.

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***. Specifically, this document tracks 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. It should be noted that this document only covers some of the obligations under FERPA and COPPA, 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 System.

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

COPPA	FERPA	Suggested 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.

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.

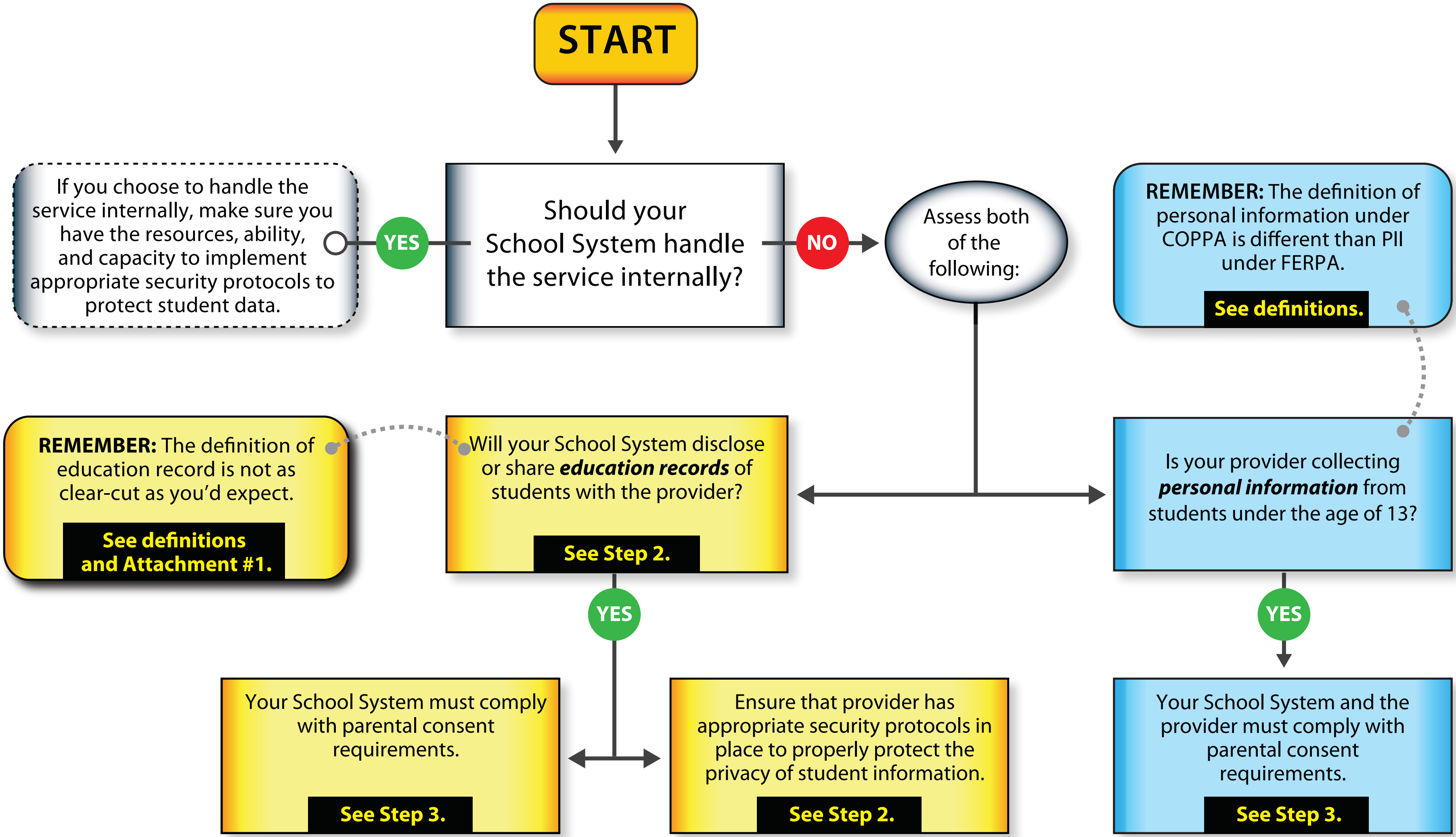
For a list of what is not considered an education record, See Attachment #1.

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



START

Should your School System handle the service internally?

YES

If you choose to handle the service internally, make sure you have the resources, ability, and capacity to implement appropriate security protocols to protect student data.

NO

Assess both of the following:

Will your School System disclose or share ***education records*** of students with the provider?

See Step 2.

REMEMBER: The definition of education record is not as clear-cut as you'd expect.

See definitions and Attachment #1.

YES

Your School System must comply with parental consent requirements.

See Step 3.

Ensure that provider has appropriate security protocols in place to properly protect the privacy of student information.

See Step 2.

Is your provider collecting ***personal information*** from students under the age of 13?

REMEMBER: The definition of personal information under COPPA is different than PII under FERPA.

See definitions.

YES

Your School System and the provider must comply with parental consent requirements.

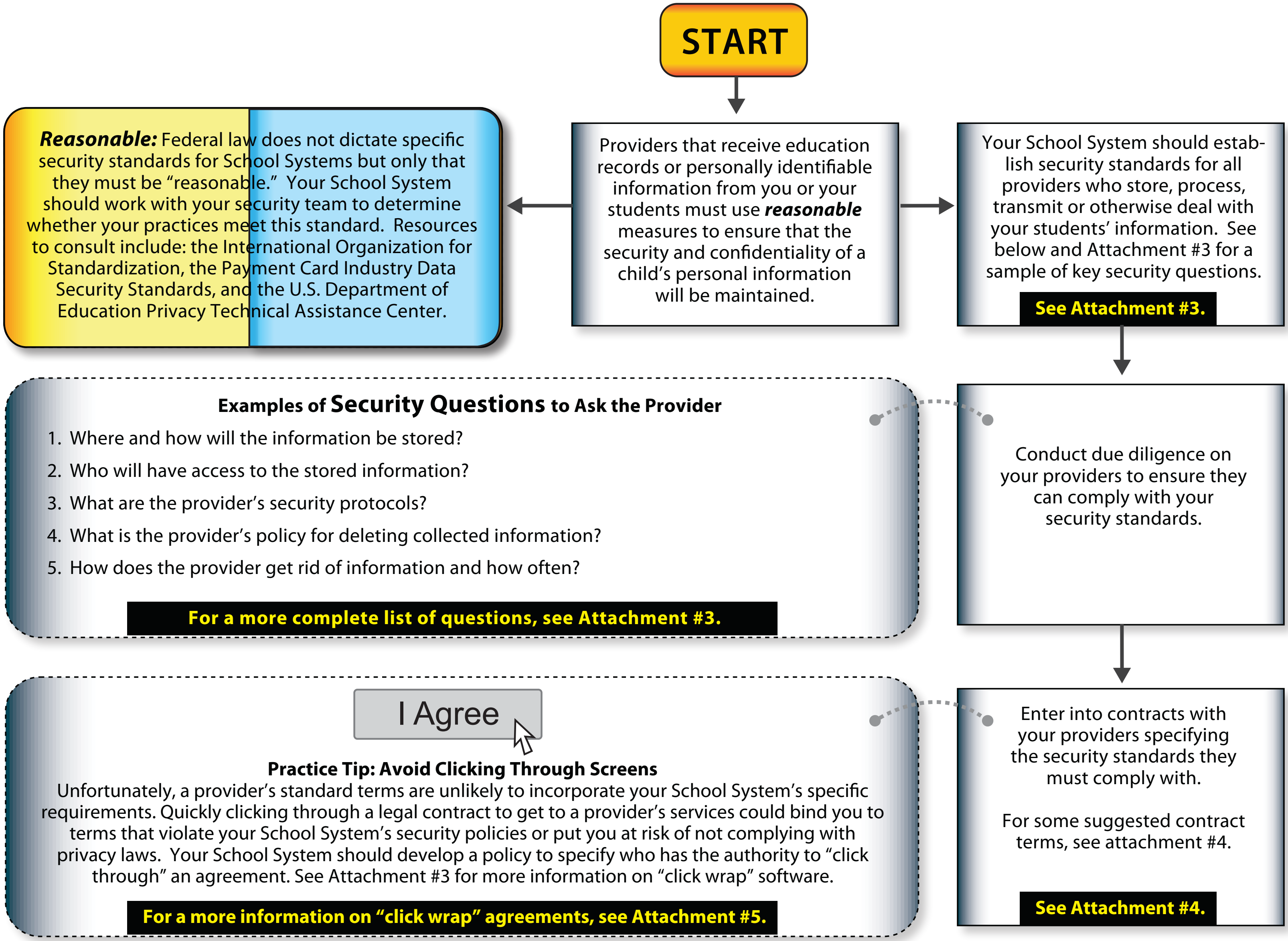
See Step 3.

Flow Chart Key

COPPA	FERPA	Suggested 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.

STEP 2: EVALUATING AND CONTRACTING WITH ONLINE SERVICE PROVIDERS



START

Providers that receive education records or personally identifiable information from you or your students must use ***reasonable*** measures to ensure that the security and confidentiality of a child's personal information will be maintained.

Reasonable: Federal law does not dictate specific security standards for School Systems but only that they must be "reasonable." Your School System should work with your security team to determine whether your practices meet this standard. Resources to consult include: the International Organization for Standardization, the Payment Card Industry Data Security Standards, and the U.S. Department of Education Privacy Technical Assistance Center.

Your School System should establish security standards for all providers who store, process, transmit or otherwise deal with your students' information. See below and Attachment #3 for a sample of key security questions.

See Attachment #3.

Conduct due diligence on your providers to ensure they can comply with your security standards.

Examples of Security Questions to Ask the Provider

1. Where and how will the information be stored?
2. Who will have access to the stored information?
3. What are the provider's security protocols?
4. What is the provider's policy for deleting collected information?
5. How does the provider get rid of information and how often?

For a more complete list of questions, see Attachment #3.

Enter into contracts with your providers specifying the security standards they must comply with.

For some suggested contract terms, see attachment #4.

See Attachment #4.

Practice Tip: Avoid Clicking Through Screens

Unfortunately, a provider's standard terms are unlikely to incorporate your School System's specific requirements. Quickly clicking through a legal contract to get to a provider's services could bind you to terms that violate your School System's security policies or put you at risk of not complying with privacy laws. Your School System should develop a policy to specify who has the authority to "click through" an agreement. See Attachment #3 for more information on "click wrap" software.

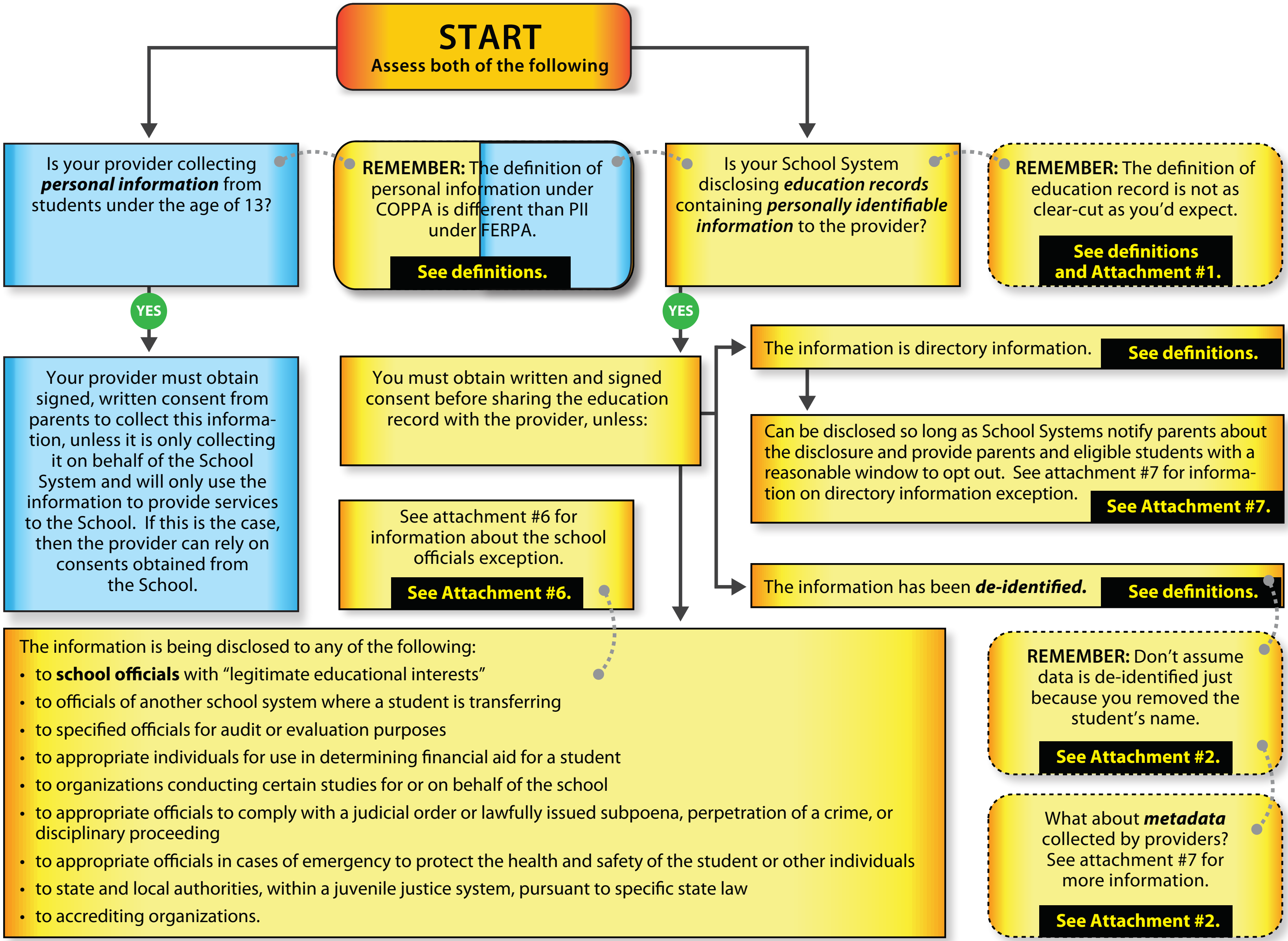
For a more information on "click wrap" agreements, see Attachment #5.

Flow Chart Key

COPPA	FERPA	Suggested 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.

STEP 3: PROVIDING NOTIFICATION AND OBTAINING PARENTAL CONSENT



START
Assess both of the following

Is your provider collecting ***personal information*** from students under the age of 13?

REMEMBER: The definition of personal information under COPPA is different than PII under FERPA.

See definitions.

YES

Your provider must obtain signed, written consent from parents to collect this information, unless it is only collecting it on behalf of the School System and will only use the information to provide services to the School. If this is the case, then the provider can rely on consents obtained from the School.

Is your School System disclosing ***education records*** containing ***personally identifiable information*** to the provider?

REMEMBER: The definition of education record is not as clear-cut as you'd expect.

See definitions and Attachment #1.

YES

You must obtain written and signed consent before sharing the education record with the provider, unless:

The information is directory information. **See definitions.**

Can be disclosed so long as School Systems notify parents about the disclosure and provide parents and eligible students with a reasonable window to opt out. See attachment #7 for information on directory information exception. **See Attachment #7.**

The information has been ***de-identified.*** **See definitions.**

REMEMBER: Don't assume data is de-identified just because you removed the student's name.

See Attachment #2.

What about ***metadata*** collected by providers? See attachment #7 for more information.

See Attachment #2.

See attachment #6 for information about the school officials exception.

See Attachment #6.

The information is being disclosed to any of the following:

- to **school officials** with "legitimate educational interests"
- to officials of another school system where a student is transferring
- to specified officials for audit or evaluation purposes
- to appropriate individuals for use in determining financial aid for a student
- to organizations conducting certain studies for or on behalf of the school
- to appropriate officials to comply with a judicial order or lawfully issued subpoena, perpetration of a crime, or disciplinary proceeding
- to appropriate officials in cases of emergency to protect the health and safety of the student or other individuals
- to state and local authorities, within a juvenile justice system, pursuant to specific state law
- to accrediting organizations.

Flow Chart Key

COPPA | FERPA | Suggested 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.

#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.

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.

#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.

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.

#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.

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.)?

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?

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 HTPPS?

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.

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.

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?

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 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)?

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?

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 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 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 be responsible for complying with COPPA.
    - The provider should be liable for any violation of COPPA, FERPA, or any other applicable laws, caused by the provider.
    - The provider should be liable for any breaches in security or unauthorized third party access arising out of the provider's negligence.
    - The provider should indemnify the School System for any claims or damages that arise out of the provider's negligence, and the provider's failure to comply with COPPA, FERPA, or other applicable laws.
    - All liability described in this list should be uncapped.
    - The School System should also consider whether this type of liability should be excluded from traditional disclaimers 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 look out 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.

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.

#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.

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

Collaborating Organizations

- Harvard Law Clinic 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:

David Bein, SFO, Assistant Superintendent of Business Services	East Maine School District 63
Shirley Broz, Retired - Former Director of Technoloy	Rockwood School District, Murrieta, CA
Robert L. Clayton, Counsel	Gonzalez Saggio & Harlan LLP
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
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

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.