

CoSN Student Data Privacy Toolkit



PART 2

Partnering with Service Providers



About CoSN

The Consortium for School Networking (CoSN) is the premier professional association for school system technology leaders. CoSN provides thought leadership resources, community, best practices and advocacy tools to help edtech leaders succeed in the digital transformation.

Table of Contents

1.	Introduction.....	4
2.	Toolkit Definitions.....	5
3.	Vetting Online Educational Services.....	6
i.	Different Approaches to Vetting Online Services.....	6
ii.	Creating Context for the Vetting Process.....	8
4.	How to Read a Privacy Policy.....	14
5.	Understanding Metadata, Pseudonymous Data, and De-identification.....	20
6.	Security Questions to Ask of An Online Service Provider.....	22
7.	Contracts and Terms of Service.....	25
8.	Due Diligence for “Click-Wrap” Software.....	30
9.	Communicating Your Decisions.....	32
10.	Next Steps.....	32
11.	Acknowledgements.....	33

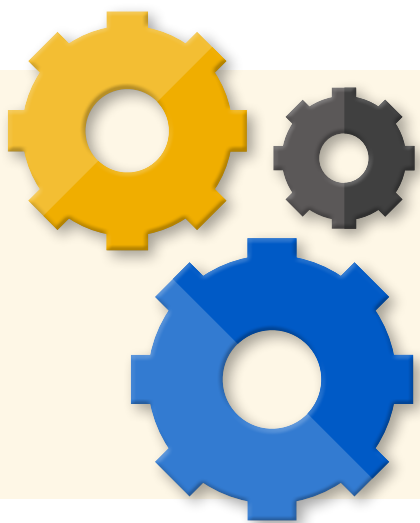
Introduction

CoSN's Student Data Privacy Toolkit has been designed to help School Systems understand and implement foundational practices to support protection of student personally identifiable information. The work of privacy is never done. Instead, it is a continuum of ongoing attention and improvement, ever expanding and maturing to build stronger protections over time.

A key component of that work is understanding and managing the ecosystem of external service providers that are brought into a School System or that are otherwise provided with access to information about students. These Providers are as diverse as the School Systems they support and the services they provide, which include supports for education, efficiency, and infrastructure, as well as extra-educational services including social and emotional supports from community organizations, athletics, and more.

This Section Two of the CoSN Student Data Privacy Toolkit is focused on helping School Systems approach their work with Providers with confidence and competence, with an aim toward demystifying certain language and practices to better position School Systems to achieve their goals.

If you've not yet reviewed Section One of the CoSN Student Data Privacy Toolkit, "Student Data Privacy Fundamentals," we encourage you to do that first. Section One provides an overview of common federal student data privacy laws with which School Systems and Providers must comply, as well as discussion of state student data privacy laws. This Section Two provides guidance for School Systems on approaches to applying that information to evaluation of online educational products and services.



The work of privacy is never done. Instead, it is a continuum of ongoing attention and improvement, ever expanding and maturing to build stronger protections over time.

Toolkit Definitions

We use the following terminology across the Student Data Privacy Toolkit:

- **School System:** an educational agency, including a school, district, or other local education agency
- **Student Data:** any student information that is protected under applicable federal or state privacy law, including information that identifies, relates to, describes, could reasonably be associated with or could reasonably be linked, directly or indirectly, with an individual student. Student Data is also referred to as personally identifiable student data or student personally identifiable information.
- **Provider:** a technology company, community service provider, or other School System partner that has access to Student Data.
- **Privacy:** practices governing the collection, use, handling, disclosure, and deletion of Student Data, with a primary focus on the individual's personal right to be free from intrusion.
- **Security:** protections designed to preserve the confidentiality, integrity, and availability of Student Data and to prevent unauthorized access to and disclosure of Student Data.
 - **Privacy** and **security** are related disciplines, but they are not interchangeable. Both a privacy program and a security program are needed to properly protect Student Data.



Vetting Online Educational Services

As discussed in Section One of the CoSN Student Data Privacy Toolkit and as suggested by the definition of Privacy that we've included above, building and implementing a privacy program is focused on protecting individual rights and managing both individual and organizational risk. The work must be focused on School System policies and practices in order to support consistent, cross-team organizational behaviors and build strong internal privacy protections. This inward focus also helps to establish School System expectations for protecting Student Data when it is shared with Providers, including online educational service Providers.



Ensuring the protection of Student Data when it is shared with Providers requires that the School System understand Provider privacy practices. This is typically done by vetting Provider products or services prior to engaging in a contract with the Provider.

Once the vetting process has been completed, the next steps are to engage in a well-informed contract with the Provider, and to communicate requirements for using the Provider's products or services, including any associated restrictions, within your School System.

Different Approaches to Vetting Providers

There is no "one-size-fits-all" approach to vetting Providers, and no tool or service that can do it for you. Assessing the suitability of your Providers is a risk-mitigation exercise, and it is dependent on your School System's interpretation of legal requirements, your School System privacy program policies, community expectations, and of course, levels of risk tolerance.

No one can tell you that a Provider's product or services is appropriate, lawful, and acceptable for use in your School System except those in a position of authority to do so in your School System and your counsel. However, there are a variety of free third party services that examine educational technology products, and leveraging the results of multiple services can help you "narrow the field" of Providers to choose from in support of your larger vetting process.

The vetting process can be complex, but it shouldn't include only the technology team. When done well, the process often starts with the curriculum team, which may assess whether or not an online product or service provides curriculum-aligned value, making it worth the work to assess for privacy and security practices.

Before beginning a privacy and security assessment, consider what steps your School System should take to "pre-qualify" a Provider's product or service for privacy and security review. Considerations might include curriculum, finance, or other facets, any of which might disqualify it from being reviewed by the technology team.

Once a product or service has been qualified for a privacy review, some common approaches to vetting the products and services offered by online educational Providers include:

1. Read the Provider's applicable privacy policy and terms of use or service.
 - a. This is the minimum standard and the most common approach across School Systems. Reviewing this documentation should help you understand what Student Data the Provider collects, uses, and discloses, and how the privacy of that Student Data is protected.
 - i. Be sure you are reviewing the applicable privacy policy and terms. That is, the review must be of the documentation that applies to the product or service, not to be confused with the documentation that applies to a consumer website if it is not implicated in collection of Student Data.
 - ii. Based on the sensitivity of the Student Data being disclosed and how it is used, you may need to request additional details on the Provider's security practices.

This process should help you understand the Provider's fundamental privacy practices. However, it is not a thorough review, and you may find that reviewing the documentation is not always sufficient to gather the information that you need in order to make a decision about the appropriateness of the product or service.

2. Read the Provider's applicable privacy policy and terms of use or service, and compare the findings with what you can see via an examination of the product or service.
 - a. Combining the review discussed above with use of the product or service should help you to verify the accuracy of the privacy policy, at least for the collection of Student Data that is readily apparent. For example, if the privacy policy notes that the product does not require creation of an account, or if only certain data fields are required in order to create an account, this is easily verified by accessing the product.

Getting more familiar with the Provider's product or service supports a deeper understanding of Student Data practices, and can also help to clarify statements in the privacy policy.

There are, of course, deeper and more complex methods of vetting online products and services, typically involving a technical assessment leveraging open source tooling. However, these methods are more time-consuming and although highly recommended, use is not widespread in education.

Note: See Security Questions to Ask of an Online Service Provider for information on the security component of the vetting process.

Creating Context for the Vetting Process

When evaluating the use of Student Data against the potential risks, it is helpful to consider the categories of data an application uses, the source of the data and sensitivity of the Student Data. Understanding these facets helps to create proper context for your assessment of the privacy practices.

Categories of Student Data: What Student Data elements are collected? Does it constitute education records? Does it include sensitive data, such as financial, behavioral, medical, socio-economic, biometric data, and IEP plans?

Sensitivity: Not all products and services have or need access to highly sensitive data, and some School Systems have developed **Data Classification** frameworks to provide guidance when evaluating the risk of disclosing data to a Provider. Developing a classification system also helps to inform the levels of protection that a School System should have in place around the data it has on hand and is leveraged to assess rules about what types of data might be shared both within and outside of the School System.

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

Student Data and Education Records in the Absence of a Student Account

A common misconception among some School Systems is that if a product is intended for use directly by students, but students are not required to create an account to use the product, that no Student Data is shared. Think again!

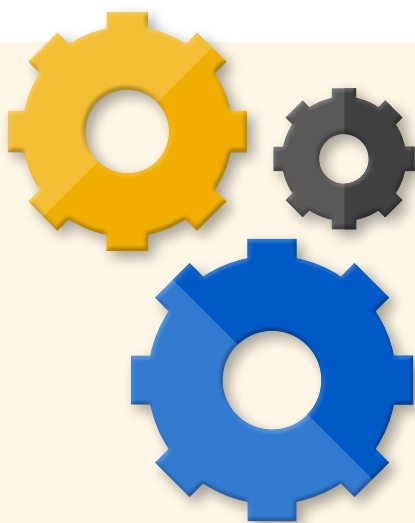
If tracking technologies are used, such those that are commonly integrated by a Provider to understand how its product is being used, troubleshoot issues, and maintain security, it is possible that Student Data—perhaps in the form of an IP address or User ID—is being shared. In addition, if a student can use a product and have their progress saved, that also indicates that Student Data is being shared and an Educational Record is likely being created.

Be sure you understand what is happening even in the absence of a student account so that you are able to make a well-informed decision about the product. Even if the Student Data being shared is quite limited, your School System still has legal obligations to consider. Also review your state law requirements carefully, as many have broad definitions of Student Data that would encompass the type of information described above.



Sources of Student Data: How does the Provider collect the Student Data? For example, is it provided:

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



Not all products and services have or need access to highly sensitive data, and some School Systems have developed Data Classification frameworks to provide guidance when evaluating the risk of disclosing data to a Provider.

Vetting Online Tools: Start with Privacy

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

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

Application Vetting: An Overview

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

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



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

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



Communicate the decision to teachers, students, and parents.

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

Continues.

Is Student Data Being Disclosed to a Provider?

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

- When dealing with Education Records protected by FERPA, parental consent is required unless an exception applies.
- The most common exception when working with Providers is the School Official exception.
- What is or is not an Education Record is not always clear-cut.
- Be sure to assess with your School System's legal counsel whether or not the Student Data is being collected, generated, stored, or otherwise processed by a Provider qualifies as an Education Record before proceeding.
- Be mindful that any disclosure of Student Data to a Provider using the Directory Information exception of FERPA might lead to creation of an Education Record, for which you must have "direct control," which is not available when Student Data is released as Directory Information.
- Will students be asked to disclose sensitive information protected by PPRA?
- Ask the Provider and review the product or service to determine if any other sensitive Student Data is collected (such as biometric data).

Will the Provider Collect the Student Data Directly From Students?

If YES, also consider PPRA and COPPA.

- PPRA applies when collecting Student Data from students on certain sensitive subjects or when Student Data will be used for marketing purposes.
- COPPA applies when Student Data is collected online by commercial Providers from children under age 13.
 - Pay attention to any language in a Provider's terms of use or service that prohibit use of the product by children under age 13, or that delegate responsibility for obtaining consent to the School System.

Continues.

Is Parental Consent Required to Disclose Student Data to the Provider?

If YES, consider PPRA and COPPA.

- PPRA requires parental notification and an opportunity to opt-out when Student Data is collected from students for marketing or sales purposes. These practices may also be prohibited under your state laws.
- COPPA consent, for students under age 13, is described below.

IF the School System is contracting with the Provider and Student Data is used for the benefit of the students and School System, the School System may choose to provide consent on behalf of the parent, and the Provider may rely on the contract as indicative that the School System has managed the consents.

OR

IF the Provider collects, uses, or discloses Student Data for commercial purposes not related to the provision of the services requested by the School System, the School System may not provide the consent.

Will the Student Data be Used for Marketing Purposes, and not for the School Purpose?

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

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

Continues.

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

- What Student Data is collected from the School System and from students?
- Is Student Data collected by or disclosed to third parties?
- How is the Student Data used?
- How is the Student Data protected?
- How long is the Student Data retained?
- How does the School System access its Student Data?
- What happens to the Student Data when the agreement ends?
- Is notice given before changes are made to the Privacy Policy?

Does the Provider's Privacy Policy and Terms of Use and/or Services or other Contract Provide Sufficient Assurances to Make an Informed Selection?

If YES, and your vetting process has been completed successfully, with no adverse findings, communicate the decision to teachers, students, and parents.

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

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

How to Read a Privacy Policy

In order to consider whether a product or service is appropriate for use in your School System, a minimum requirement is to review the Provider's Privacy Policy.

The Privacy Policy (sometimes called a privacy notice) is used to inform the users of a product or service what personally identifiable information the Provider collects and how it may be used, shared and retained.

The Privacy Policy is a legal requirement. It must be truthful, and accurately reflect the data practices. It is not intended to list the types of personally identifiable information a Provider doesn't collect. However, if personally identifiable information is collected and not disclosed in the Privacy Policy, or if there are other misleading or deceptive statements (or absence of such statements) in the Privacy Policy, the Provider could be subject to regulatory action under Section 5 of the Federal Trade Commission Act.

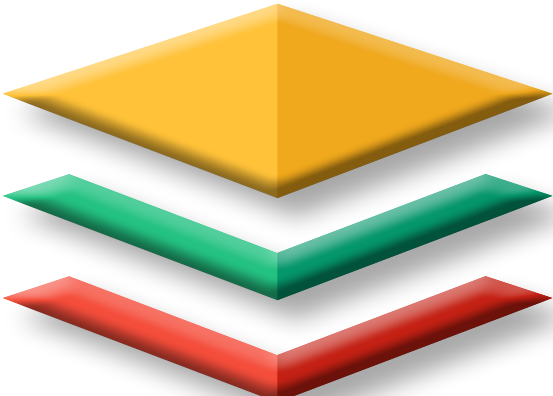
If there is no available privacy policy for the online product or service you are considering, it is advisable to find an alternative product or service to be used within your School System.

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

Considerations When Reviewing a Privacy Policy

Questions	Explanation
General Questions <ul style="list-style-type: none"> Is the privacy policy easy to find and available before the collection of any personally identifiable information? Is it clear which products or services are covered by the policy? Does the policy state when it was last updated? Is it written in a clear and understandable manner? 	<p>The privacy policy should be available in advance of any decision to use the product, and should be available to all users. It should be clear what products and services it applies to, and should identify when it was last changed. While there are sometimes areas of a privacy policy that may be stated in legal language, as with all legal documents, be sure you understand it.</p>

Continues.

Questions	Explanation
<p>What Personally Identifiable Data is Collected?</p> <ul style="list-style-type: none"> • What personally identifiable data is disclosed to the vendor from the School System (e.g., to create accounts)? • What personally identifiable data does the Provider collect from users? • What, if any, metadata* is collected or generated by the vendor, either directly or by third parties through technologies such as via cookies, plug-ins, web beacons, etc.? 	<p>The privacy policy should explain what personally identifiable information is collected and how. (For example, is the personally identifiable information provided by the School System, the individual user, or collected passively through the use of various technologies?)</p> <p><i>*Note that sometimes metadata is not personally identifiable.</i></p>
<p>How is the Personally Identifiable Data Used?</p> <ul style="list-style-type: none"> • Does the privacy policy explain how the Provider may use Student Data, as well as personally identifiable data from and about your School System employees? • Does it specify any limits that may apply to the Provider's use of that data? • Does the privacy policy make it clear that the Provider will only collect, store and use personally identifiable information as necessary to perform the designated services for the School System? • If applicable, does the policy address how sensitive information might be used? 	<p>Fundamental to your being able to maintain "direct control" over the Education Record as required under FERPA, is establishing what Student Data a Provider will have access to, for what purposes and how they may handle it.</p> 

Continues.

Questions	Explanation
<p>Is/How is Data Further Disclosed?</p> <ul style="list-style-type: none"> • Does the privacy policy specify what Student Data or types of Student Data might be disclosed to 3rd parties? • Does the privacy policy provide an explanation of the types of third parties that might receive that data? • Does the privacy policy explain what those 3rd parties may do with the data? 	<p>In some cases, the Provider may be disclosing information to third parties solely to provide your School System with the product or service you've requested. For example, a Provider may disclose information with a cloud service provider to store the data, or with an analytics company to develop reports to show teachers how their students are progressing in the product. In other cases, the intended use may go beyond that legitimate educational interest or fundamental operation of the product.</p> <p>Consider if the contract needs to clarify whose responsibility it is (the Provider's or the School System's) to obtain parental consent when the intended use may go beyond that legitimate educational interest or basic product operation, or whether such use is permissible under your state student data privacy law.</p>
<p>Data Access</p> <ul style="list-style-type: none"> • Does the privacy policy specify whether the School System and/or parents (or eligible students) will be permitted to inspect and request to amend records as specified in FERPA? • If access to inspect the records is not available directly to the School System and/or parents (or eligible students), does the privacy policy explain how the Provider will facilitate such access if requested? • Does the privacy policy make it clear what the process would be to obtain such access? 	<p>Under FERPA, School Systems are required to respond to requests from parents and eligible students to inspect and request to amend certain information in the Education Record. Be sure you understand how you will manage such requests when the data is held by a Provider.</p>

Continues.

Questions	Explanation
Data Security <ul style="list-style-type: none"> Does the privacy policy provide basic information about the data security practices? Based on the Data Classification of the information stored and any associated risks, does the privacy policy provide sufficient information about the data security practices to assess whether the protections are sufficient? 	<p>The privacy policy does not typically detail security measures, so consider whether or not the privacy policy notes that the security practices are consistent with “standard industry practices” or “commercially reasonable measures.” If you have specific security requirements for your data, assess whether or not these considerations are addressed or if you need to request additional information from the Provider.</p>
Data De-identification <ul style="list-style-type: none"> Does the privacy policy explain if the Provider will de-identify Student Data, and what that de-identified data will be used for? Does the privacy policy include language that suggests an understanding of the FERPA de-identification standard? 	<p>It is fairly common for Providers to want to use de-identified data. FERPA has a very high standard for de-identification, and you may want to consider whether or not the Provider’s privacy policy, terms, click-wrap or formal contract refers to that standard or suggests that the Provider understands that obligation.</p> <p>In addition, many state laws restrict the use of de-identified data. Refer to your state laws to ensure that the Provider’s use cases align with your understanding of the regulatory requirements, particularly when those cases do not clearly fall within the bounds of the education purpose.</p>



Continues.

Questions	Explanation
<p>Data Retention and Disposal</p> <ul style="list-style-type: none"> Does the privacy policy address how long the Student Data and other personally identifiable information will be maintained? Does the Provider intend to retain de-identified data? 	<p>Personally identifiable data disclosed to the Provider, or collected by the Provider during the use of the product or service should be destroyed by secure means within a reasonable time frame after it is no longer necessary for the purpose for which it was provided or at termination or expiration of the contract. (See Best Practices for Data Destruction from the US Department of Education's (ED) Privacy Technical Assistance Center (PTAC).)</p> <p>Consider any state or local records retention laws or policies, which may have specific requirements about when Student Data must be deleted.</p> <p>Note also, that some state laws give students certain rights to receive their user-generated data if the Provider maintains user accounts.</p> <p>You should also understand whether or not de-identified information will be retained.</p>
<p>Changes</p> <p>Will the Provider give notice and provide the opportunity for the School System to consent before making material changes to the Privacy Policy?</p>	<p>What constitutes "material" change is a legal threshold question, but it commonly refers to changes that involve using or disclosing personally identifiable information in a new way, different from the original purpose for which it was collected, or changes that adversely impact the privacy or security of the data. Under these circumstances, the Provider is legally required to provide notice and obtain consent to the changes.</p> <p>Non-material changes may include changing the Privacy Policy to make it easier to read, improving privacy and security protections or explaining a new feature that does not include using already collected data in a new way. These types of changes generally require notice, but not consent.</p>

Continues.

Questions	Explanation
Contact Does the Privacy Policy provide a contact for privacy related questions?	Be sure you understand how you can contact the Provider if you have questions about the Privacy Policy.

What is Reasonable Security?

As you may have noticed, privacy laws often refer to a requirement to implement “reasonable” security. This tends to be an area of confusion for some School Systems, but it does have meaning.

“Reasonable” is a term of art in the law. In practice, “reasonable security” is often the yardstick the Federal Trade Commission (FTC) uses when bringing enforcement actions against companies that have implemented lax security practices (typically seen in settlements with companies after a data breach) or when a company has misrepresented its security practices. As such, there is some meaning and weight behind a Provider’s use of the phrase.

A simple, [starter guide to “reasonable security” is available from the FTC](#). It by no means covers all the practices that FTC has cited in its enforcements, but it is a good, plain-language starting point.

When done well, Privacy Policies should be easy to understand. However, that’s not always the case. Take the time to work through a few, and be assured that—as with most new projects—it gets easier with time and experience. When in doubt, reach out to the Provider and ask the questions about their Privacy Policy that you need answered.



Understanding Metadata, Pseudonymization, and De-identification

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

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



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

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

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

Once the data has been de-identified, ED notes that it may be released without parent consent.

However, the standard for de-identification under FERPA is quite complex, and whether or not data is considered to be de-identified may change, depending on how different data elements may be combined. In many ways, de-identification of data is its own science, and whether or not a data set has been de-identified depends in part on the context. Before you disclose de-identified data, consider engaging with competent experts to review your de-identification standards.

In addition, ED's former Chief Privacy Officer Kathleen Styles cautioned, "re-identification risk is a very real risk. You can't just take off somebody's name... With the amount of information that's available online, it's increasingly easy to re-identify individuals."

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

Pseudonymized vs Anonymized Data

Pseudonymization refers to a process in which certain identifiers in a data set are replaced with fictitious data. Note that pseudonymized data is not de-identified. It is a risk mitigation strategy, but it is not wholly de-personalized data.

Anonymized data is a process by which the data has been sanitized to the point of not being able to be re-identified. Anonymization is the strongest of the practices, but it is very difficult to achieve and is not common practice.

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



Security Questions to Ask of an Online Service Provider

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

While most privacy laws do not prescribe specific security standards, regulatory guidance often refers to "reasonable security methods." According to ED, methods are usually considered reasonable "if they reduce the risk to a level commensurate with the likely threat and potential harm." The greater the harm that would result, the more protections a School System must use to ensure that its methods are reasonable.

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

The following is a non-exhaustive list of key security questions to discuss with your Provider to help better understand how they manage security of Student Data. Although the questions below deal with Student Data, you may wish to ask these questions in relation to all personally identifiable data that will be shared with the Provider.



Network Operations Center Management and Security

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

Continues.

Student Data Storage and Access

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

Availability

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

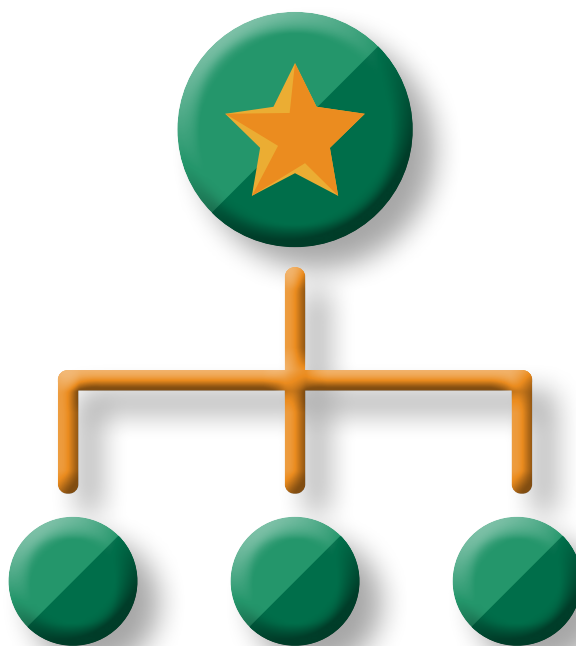
Continues.

Audits and Security Standards

- Does the Provider give the School System the ability to audit the security and privacy of its records?
- Has the Provider engaged with a third party to audit its security operation?
- Does the Provider align with a recognized security standard such as the International Organization for Standardization (ISO) or the National Institute of Standards in Technology (NIST)?

Data Breach, Incident Investigation and Response

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



Contracts and Terms of Service

Once the vetting process has been completed, and your School System has decided that the product or service in question is appropriate for use in your School System, the work turns to addressing the contractual agreement between the School System and the Provider.

The contract should specify how the Provider will manage their responsibilities including compliance with applicable laws and any additional privacy and security practices required by your School System.

To get started:

Review the Provider's agreements that outline the responsibilities between the Provider and the School System. Depending on the product or service, this may be a formal contract, terms of service, or a "click-wrap agreement." Based on what you have identified in the review of the Privacy Policy, security practices and terms, and any testing you may have conducted on the product or service, determine whether or not you need to negotiate new or additional terms with the Provider.

If negotiation is not possible, find an alternative product or service with a Provider who will engage in constructive negotiations with your School System.

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

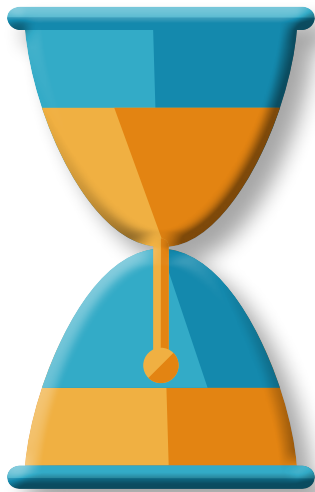
Considerations for Contracts and Terms of Service

Topic	Explanation
Services and Purpose Describe the product or service being provided. If applicable, specify that the Provider is designated as a School Official, describe the legitimate educational interest that the Provider is fulfilling, describe the nature of the Student Data to be collected, and the purpose for which any personally identifiable information from Education Records is being disclosed.	If you have determined that the Provider qualifies as a "school official" under FERPA, this establishes the conditions under which you are disclosing the personally identifiable information from Education Records. This summary description may also be useful in writing a notice to parents describing the online services used by the School System.

Continues.

Topic	Explanation
<p>Contract Scope</p> <p>Identify all elements that comprise the agreement and any contract terms that are incorporated by reference (e.g., the Provider's Privacy Policy) and what order of precedence is followed in the event of a contradiction in terms.</p>	<p>A Provider's terms (or the products themselves) may contain links to documents that could be updated over time, and/or may contain language that contradicts the agreement between the Provider and the School System. Defining the order in which terms are to be interpreted, when applicable, reduces the potential for misinterpretation.</p>
<p>Data Collection, Use and Transmission</p> <p>Specify how the Provider may collect and use Student Data, and any restrictions that may apply to the Provider's use of that data. Be clear that the School System, and not the Provider, retains control over and rights to the Student Data.</p>	<p>Fundamental to your maintaining "direct control" required under FERPA is establishing what Student Data a Provider will have access to, for what purposes and how they may handle it. Some or all of this may already be contained within the Provider's Privacy Policy, and that can be helpful if it is incorporated into the agreement by reference. However, it is not always appropriate for the Privacy Policy to be a contractual agreement, and there may be items missing or additional details that should be added to the agreement.</p>
<p>Data De-Identification</p> <p>Specify if a Provider may de-identify any of the Student Data and if it will retain such de-identified information.</p>	<p>Consider your state law allowances and restrictions on a Provider's use of de-identified data.</p>

Continues.

Topic	Explanation
<p>Data Security</p> <p>Specify any security requirements that the Provider must follow to the extent that it maintains, processes, or stores Student Data.</p> <p>At a minimum, the contract should specify:</p> <ul style="list-style-type: none"> • That the Provider securely maintains all such records or Student Data in accordance with industry standards. • That the Provider restricts access to your School System's Student Data to only those individuals that need to access in order to perform the agreed-upon services. <p>In addition, if you require that specific security standards must be in place for certain data elements, those should also be specified in the agreement if those data elements will be disclosed to the Provider.</p> <p>Clarify whether or not you may audit the security and privacy of your Student Data, or have access to results of or summary results of third party audits.</p> <p>Require notification about changes that will adversely impact the availability, security, storage, usage or disposal of any information.</p> <p>Data collected and stored from and on behalf of one School System should be stored and maintained separately—either by physical or technical means—from the information of any other School System.</p>	<p>Ensure that the contract provides appropriate assurances about how your Student Data will be protected in accordance with School System policies relevant to the Student Data that the Provider will receive or collect.</p> 
<p>Data Breach</p> <p>The agreement should identify what happens if the Provider has a data breach that impacts your Student Data. The agreement should identify the Provider's responsibilities including required notification time, and any obligations for end user notification and mitigation.</p>	<p>The procedures should, at a minimum, follow the legal requirements, which vary by state. Most states have data breach laws dealing with financial and other sensitive information, and some have laws addressing breach of education data.</p>

Continues.

Topic	Explanation
<p>Data Retention and Disposal</p> <p>Assure the proper management and disposal of Student Data and personally identifiable employee data. All personally identifiable data disclosed to the Provider, or collected by the Provider, must be disposed of by secure means to ensure that it is protected from unauthorized access or use. Keep in mind that some School System information may need to be retained for the Provider's legal record-keeping purposes, but that should not include Student Data.</p>	<p>Consider any state or local records retention laws or policies, including rights that students may have under certain state laws to retain copies of their user-generated content in the event that the Provider supports student accounts.</p>
<p>Bankruptcy or Acquisition</p> <p>Specify what happens to the data if the Provider goes out of business or is acquired by another organization.</p>	<p>Consider if the data will remain protected under the agreed-upon contract, Privacy Policy and security policy if the vendor is acquired, or merges with another organization, or in the event of bankruptcy or dissolution.</p>
<p>Service Levels and Support</p> <p>Specify the service levels the Provider must meet and any credits you will receive for any failure by the Provider to meet those service levels.</p> <p>Require the Provider to supply the School System with the technical assistance you may need to operate the services.</p>	<p>Service Level agreements deal with expectations of availability, which along with integrity and confidentiality, is one of the three key principles of security.</p>
<p>Governing Law and Jurisdiction</p> <p>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.</p>	<p>Check with your legal counsel about what law can govern contracts entered into by your School System in light of your state laws.</p>

Continues.

Topic	Explanation
<p>Duration, Modification and Termination</p> <p>Establish for how long the agreement will be in force, and what the procedures will be for modifying the terms of the agreement (mutual written consent to any changes is a best practice). Specify what both parties' responsibilities will be upon termination of the agreement, particularly regarding disposition of Student Data maintained by the Provider. Upon termination of the contract, the Provider should return all Student Data or allow the School System to download that data, and properly delete any copies still in its possession, including archives and/or backups.</p>	<p>Agreements should govern behavior during and at the end of the term. In addition, allowing one party to modify an agreement at will puts the other party at a legal disadvantage and may jeopardize a School System's ability to retain control over the Student Data as required by FERPA.</p>
<p>Liability</p> <p>The Provider should be responsible for the activities of its staff and subcontractors.</p> <p>Both parties should have an obligation to comply with all applicable laws, including applicable state student data privacy laws, and each party should be liable for its own actions. If the Provider will be collecting data from children under the age of 13, the Provider should comply with COPPA.</p>	<p>Avoid being too broad. It is unrealistic to stipulate that a Provider comply with the entire state education code, or other laws or sections of laws that do not apply.</p> <p>It is similarly unrealistic to stipulate that a Provider assume liability for data breaches or other incidents caused by the School System. Limits of liability should appropriately allocate risk between the Provider and the School System as the owner of its data.</p>

Due Diligence for “Click-Wrap” Software

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

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

In considering a process to manage assessment of click-wrap agreements, you might establish a policy that designates which employees in your School System are authorized to click through Provider agreements. Although there are no existing federal requirements as to who in a School

System may contract with Providers, most School Systems already have such policies for paid services. In addition, when it comes to COPPA, the FTC recommends that, as a best practice, the decision about whether or not a Provider’s information practices are appropriate should be made at the district or school administration level, rather than delegating it to a teacher, noting that many schools have a process for assessing Provider practices so that the task doesn’t fall on a teacher’s shoulders.

Data Retention and Click-Wrap Software

Agreements with Providers should specify that the Student Data must be deleted. Your School System may also require return of the Education Record prior to that deletion. But what happens when you’ve engaged with a Provider under a click-wrap agreement that has no termination date? How would the Provider know when you decide to stop using the product?

When reviewing click-wrap agreements, assess the deletion schedule for Student Data to consider whether it comports with your expectations. In many cases, it may actually be your School System’s responsibility to alert the Provider when your School System is no longer using the product and request that they delete the Student Data in their care.

Partnering with teachers to create a process in which you are notified when certain products are no longer being used may be a helpful first step in allowing you to then notify a Provider of your data deletion request.

With the policy in place, provide adequate information and training to these individuals so that they can make informed decisions in evaluating the services and agreements.

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

Data Sharing Agreements

When School System requirements are missing from an agreement, particularly requirements related to Student Data privacy, School System legal counsel may create a rider in the form of a Data Sharing Agreement or Data Protection Addendum, containing the School System's minimum Student Data privacy and security requirements and obligations that Providers will need to agree to before the School System can utilize the services.

In using this approach, School Systems should keep in mind that every situation is different and it is unlikely that a single rider will work in every situation without some negotiation.

What Data Sharing Agreement Should Your School System Use?

While it's possible that your legal counsel has drafted your data sharing agreement, you may also have access to a data sharing agreement used by other School Systems, or one that was drafted by a third-party or someone else's legal counsel. The origin of the data sharing agreement is less important than the content of the agreement.

Whichever path you choose to take, be sure that your School System legal counsel has reviewed it, that you understand it, that you know how to apply it in context of different Provider products and services, and that your legal counsel has helped you to understand your boundaries of negotiation across various terms.



Communicating Your Decisions About Provider Products and Services

After a Provider's product or service has made it through your School System's vetting process and all necessary agreements have been signed, communicate your decision about any newly approved products and services to teachers and others in your school community, including parents and students.

Teachers, in particular, should have ready access to information about what products and services have been approved, what have not been approved, and if a product or service is approved but only under certain conditions.

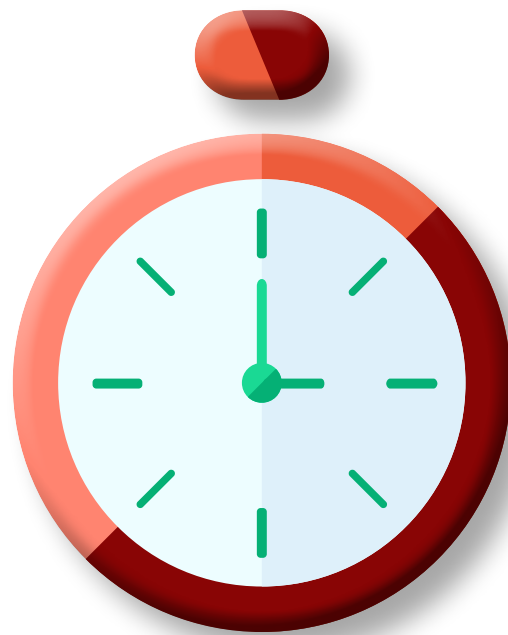
If the approval was conditional, be sure your notes on those conditions, including guidelines or instructions limiting how it may and may not be used within the School System, are clear. In addition, ensure that parents are provided with any necessary notice and the opportunity to opt-in or opt-out if such options are legally required.

Next Steps

The CoSN Student Data Privacy Toolkit consists of 3 sections, each designed to provide you with information to help support your work in protecting student data privacy:

- Part 1: Student Data Privacy Fundamentals
- Part 2: Partnering with Service Providers
- Part 3: Transparency and Trust

We encourage you to download all 3 as part of your student data privacy resource library.



Additional resources are available at CoSN.org/Privacy and below:

Useful Links

- **CoSN Initiatives:**
 - › [CoSN K12 Community Vendor Assessment Tool](#)
- **Cloud Security Alliance:**
 - › [Security Guidance for Critical Areas of Focus in Cloud Computing](#)
- **National School Boards Association:**
 - › [Data Security for Schools: A Legal and Policy Guide for School Boards](#)
- **US Department of Education Privacy Technical Assistance Center:**
 - › [Best Practices for Data Destruction](#)
- **Fordham University:**
 - › [Privacy and Cloud Computing in Public Schools](#)

Acknowledgements

CoSN would like to thank the [CoSN Student Data Privacy Educator Advisory Panel](#) for their work in creating this Toolkit. CoSN would also like to thank previous committee members, as well as Jim Siegl, Reg Leichty, Founder and Partner of Foresight Law + Policy, The Cyberlaw Clinic at Harvard Law School, Berkman Klein Center for Internet & Society at Harvard University, National School Boards Association Council of School Attorneys, and past and present sponsors of the CoSN Student Data Privacy Initiative for their work in creating the initial Toolkit and subsequent updates.

CoSN is a professional association comprised of School System 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 specificity facts and circumstances pertaining to your School System. This document does not cover all privacy law or policy. Always consult your legal counsel to understand how federal, state, and local laws and policies may apply to your School System.