The EdTech Service Provider's Guide to Student Privacy

May 30, 2025

FUTURE OF PRIVACY FORUM

The EdTech Service Provider's Guide to Student Privacy: From AI to Z

Introduction

Schools rely on education technology (edtech) service providers to manage student data and provide services and tools to help all students learn effectively. Edtech tools enhance students' learning experiences in a wide variety of ways, such as helping schools manage learning by streamlining coursework and gradebooks and using data analytics to monitor progress and provide personalized learning. These tools make learning more accessible by providing the option for virtual, independent learning as well as building solutions tailored for individual learners.

Most of these systems require online service providers to access or store student data, raising concerns about potential impacts on students' privacy. To provide solutions that harness technology's full potential in schools while protecting student data, edtech service providers must comply with, and facilitate the school's ability to comply with, the array of federal and state student privacy laws in addition to local and state contracting requirements. Because the speed of technological innovation sometimes outpaces meaningful regulation, they should also align with industry best privacy practices where existing laws are silent or unclear on certain practices. By working with schools to protect student data, service providers can help to ensure an efficient, safe, and effective learning environment for students and educators.

This Guide is designed to help online edtech service providers protect student privacy while effectively delivering educational products and services. There is no "one-size fits all" solution for ensuring data privacy–each use case must take into account the specific technology, data utilization, and underlying data governance framework. Recognizing that context matters, the Guide begins by defining the key terms and explaining the application of relevant federal and state laws to support informed conversations between service providers and education officials, and to help other stakeholders better understand the evolving education privacy landscape. It also explores how providers can go beyond legal compliance by implementing strong, transparent privacy practices that enhance both data protection and service quality, offering practical guidance for working with school districts, writing clear privacy policies, and adopting recognized best practices.

Key Terms

A clear understanding of commonly used privacy and data-related terms is essential for interpreting legal obligations and applying best practices in educational settings.

Student Personally Identifiable Information (PII)

Student personally identifiable information (PII) is a key privacy term that originates in the Family Educational Rights and Privacy Act (FERPA) (discussed below) and refers to any information that allows an individual student to be identified. This may include direct and indirect identifiers or other information that, alone or in combination, links to a specific student and could be used to identify the student. Service providers should become familiar with this term and appropriately define and use it in their policies and practices.

PII may be collected, generated, or shared in a variety of ways through educational technologies. If information is created by or about a student in an educational setting and could reasonably be linked back to that student, it should be treated as PII. In cases where identifiability is unclear, service providers should err on the side of caution and treat the data as PII unless it has been properly anonymized.

Some student PII is highly sensitive and may have additional protections under state and federal law.

Common PII Examples

Direct Identifiers

- student name
- student address
- biometric record
- email or username

Indirect Identifiers

- race and ethnicity
- dates of birth
- grades, test scores, attendance, or disciplinary records
- special needs
- posts on or work submitted through online platforms
- work performed through an educational program or app

Metadata

Common Examples

- timestamp of student login or activity completion
- performance data such as duration spent on a task and number of attempts
- tracked interactions such as resources clicked
- cursor movements or pauses during an interaction
- device type or browser used to access the platform
- location information

Metadata is data that provide meaning and context to other data. In educational settings, metadata helps interpret how students interact with digital tools—for example, patterns of engagement with content. Although metadata is often technical and indirectly related to student performance, it can still raise privacy considerations depending on whether the data can be linked to an individual.

In 2014, the Department of Education issued guidance clarifying that identifiable metadata—metadata containing direct or indirect identifiers that can be tied to an individual student—fall under FERPA protections. By contrast, metadata that have been stripped of all such identifiers are not considered personally identifiable information (PII) under FERPA and are not subject to its restrictions.

When metadata can reasonably be associated with an identifiable student, it must be handled with the same care and protections as other student PII.

Education Records

Under the Family Educational Rights and Privacy Act (FERPA), education records are defined as records maintained by an educational agency or institution (or a party acting on their behalf) that contain information directly related to an individual student.

Most student data that service providers receive from schools or collect as part of contracts with schools are part of students' education records. However, if a provider collects PII from a student when the provider is not working on behalf of a school, such as when an individual interacts directly with a service and the school is not involved, that information is likely not part of an education record even if it is personal information from an individual who is a student. Understanding what qualifies as an education record is important since FERPA's requirements apply only to information that is part of the education record maintained by a school or a third party acting on the school's behalf, and not to other student PII.

Common Examples

- grades and progress scores
- attendance and disciplinary records
- special education services or accommodations
- login records, usage logs and performance data within an online system
- communication between students and educators stored within an online tool
- student-generated work submitted through online platforms

Federal Privacy Laws Governing Edtech

Federal student privacy laws affect how online service providers collect, use, and share student data. Specific exceptions within these laws support the work of service providers, schools and districts while helping ensure compliance.

Children's Online Privacy Protection Act (COPPA)

The **Children's Online Privacy Protection Act (COPPA)** establishes rules for the collection and use of children's data by commercial websites and online services that are directed to children or with actual knowledge that they are collecting, using, or disclosing children's information. COPPA is enforced by the Federal Trade Commission (FTC) and state attorneys general, which have the power to investigate complaints, require violators to change their practices, levy fines, and enter into settlements.

COPPA requires covered services to obtain verifiable parental consent before collecting personal information from children under the age of 13. Service providers (referred to as Operators under COPPA) are subject to the law when they either direct their services to children or have "actual knowledge" that children under the age of 13 use their services. COPPA-covered services must meet certain requirements, including maintaining a clear privacy policy, directly notifying parents about data collection, and obtaining verifiable parental consent before collecting information from children under 13, not collecting more data than needed, and retaining the data only as long as necessary. Service providers may not state in their privacy policies or anywhere else that schools are responsible for complying with COPPA.

If a provider collects **only** a personal identifier and no other personal information, and is going to use a child's information only for specific internal operations no direct notice or consent is required.

COPPA gives service providers latitude in the specific way in which they obtain verifiable parental consent (VPC), so long as the way that consent is received is reasonably calculated to ensure that the person providing consent is the child's parent. For an overview of the current pre-approved VPC methods see this FPF infographic.

According to the FTC, when schools contract with a service provider, the schools may stand in for parents and provide consent for the collection of student data from children under 13. However, schools' authority to consent on behalf of parents is limited to the educational context, when providers collect personal information from students for the schools' use and for no other commercial purpose (including contextual advertisements). To obtain consent from schools rather than parents, providers must provide schools with the notices required by COPPA. The COPPA rule was updated in January, 2025, FPF has created a red-line of changes from the previous version of the rule. For more information, see the Federal Trade Commission's guidance on how to comply with COPPA.

Family Educational Rights and Privacy Act (FERPA)

Information in students' education records is governed by the **Family Educational Rights and Privacy Act (FERPA)**, a federal law enacted in 1974 that guarantees parents' right to access their children's education records and restricts who can access and use student information.

FERPA is the primary federal student privacy law. It applies to schools that receive funding from the US Department of Education, which includes K-12 public schools and most post-secondary institutions, both private and public. FERPA grants parents and eligible students the right to access and seek to correct information in students' education records. It also prohibits schools from sharing information in education records without consent, except in certain circumstances outlined in the law. Although FERPA does not directly apply to service providers, they should take time to learn its specific requirements because student records that the provider receives from a school are subject to FERPA. To support the school's compliance, service providers should be familiar with the following aspects of FERPA:

FERPA Exceptions

FERPA requires prior written consent before any PII is disclosed from a student's education record, unless the disclosure falls under one of the law's established exceptions. While the School Official Exception is the most commonly used when schools engage online service providers, it is important to be familiar with other exceptions that may also be applicable.

School Official Exception

The School Official Exception allows schools to disclose information from education records to a third party without prior consent, provided the third party is acting on behalf of the school and performing an institutional service or function for which the school would otherwise use its own employees. To qualify, the school must ensure that the third party has a legitimate educational interest in accessing the data and that the data remains under the school's direct control throughout the relationship. "Direct control" is a key concept under FERPA and is defined further in the Key FERPA Components section of this guide.

The terms "school official" and "legitimate educational interest" are not defined in the statute but must be determined by the school and disclosed to parents and eligible students in the school's

annual FERPA notification. As a best practice, schools and service providers should document how these terms are defined and operationalized within the service contract–but under FERPA, it is incumbent upon the school to determine how the school wants to define school officials and if that definition applies to the service provider.

To remain in compliance with FERPA under the School Official Exception, schools must ensure that service providers:

- Use FERPA-protected information only for the educational purpose defined in the contract.
- Do not create student or parent profiles for advertising or other commercial purposes.
- Do not collect more information than is necessary to fulfill the educational function.
- Do not share information from education records, except with approved subcontractors who are directly supporting the contracted services—and only under terms that uphold the same privacy and security commitments.

Although FERPA allows schools to delegate certain functions to outside entities, the law remains strict—and at times ambiguous—about what those entities may do with student data. Online service providers designated as School Officials must understand their responsibilities and limitations under this exception and work closely with districts to ensure ongoing compliance.

Directory Information Exception

The *Directory Information Exception* allows for the sharing of designated data without prior consent, but does require schools to provide an option to opt-out of sharing this data. Directory information is defined as "information contained in the education records of a student that would not generally be considered harmful or an invasion of privacy if disclosed." Education institutions determine which categories of information they consider to be directory information and are required to announce these categories every year. Common examples include students' names, addresses, email addresses, grade levels, weight and height of athletes, and unique identifiers such as student IDs. However, online service providers rarely receive information through this exception because once directory information is combined with non-directory information–such as student performance in a math game or search terms within a school's learning management system–it no longer qualifies as directory information under FERPA. Additionally, if a student has been opted out of directory information disclosures, they may not use tools that rely solely on this exception.

Studies Exception

The *Studies Exception* applies to studies conducted on behalf of schools for narrowly defined educational purposes, such as validating or administering assessments or enhancing instructional practices. To qualify under this exception, the school must enter into a written agreement with the organization conducting the study. This agreement must specify the purpose, limit the use and access of the data to individuals with legitimate interests, and require that the data be destroyed when no longer needed for the study. Importantly, this exception does not cover research initiated solely by an online service provider for its own purposes. Service providers conducting independent product research or analytics should not assume their work meets the requirements of the Studies Exception without a formal agreement and alignment with these conditions.

Judicial Order Exception

Although the *Judicial Order Exception* is designed to allow schools to comply with judicial orders and subpoenas, it does establish required actions when complying. Specifically, the district or school must make a "reasonable effort to notify the parent or eligible student of the order or subpoena in advance of compliance" unless the school has been ordered to not disclose the subpoena. Service providers designated as School Officials must be aware of this obligation and work with the school to provide any information ordered under a judicial order or subpoena. Furthermore, if a service provider is issued a subpoena for data under the direct control of the school, they should work with the school to ensure FERPA requirements are met.

Health and Safety Emergency Exception

The *Health and Safety Emergency Exception* provides for the disclosure of student information by the school or district (or their properly authorized representative) to appropriate parties in order to protect the health or safety of the student or other individuals. This exception should be carefully considered when establishing contract language regarding the release of student information in response to services offered through school safety platforms. This exception is limited to the period of the emergency and generally does not allow for a blanket release of PII from a student's education records. Furthermore, the emergency must be directly related to a specific student and must be related to an actual, impending, or imminent emergency. Any disclosure under this exception must be properly documented in the education record. As this expectation requires designated school officials to make a determination of a health and safety emergency, it is important for service providers to understand their role under this exception.

More information about the FERPA Exceptions is available at the Department of Education's Privacy Technical Assistance Center's website.

Key FERPA Components

FERPA establishes a framework of core requirements that govern how student education records are handled. These components define schools' responsibilities and clarify the rights of parents and eligible students. Understanding these principles—such as Direct Control, Parent Access, No Waiver of Rights, and Enforcement—is essential for service providers working with student data.

Direct Control

If a school shares student data with a service provider through the "school official" exception, the school by law maintains ownership of the education record. In this case, the service provider is considered to be standing in for the school and may use student data only for the purpose for which it was disclosed. FERPA prohibits the redisclosure of student PII from an education record, unless the disclosure is with a subcontractor that is similarly limited in how it can use the data. If a district or school directs a service provider to correct or delete information in a student's education record, they must do so and require subcontractors to do so as well. FERPA does not require a written agreement in order to disclose information from education records to school officials, but it is considered best practice to have an agreement that includes data privacy provisions. Service providers should ensure that written agreements allow for districts to maintain direct control of all identifiable data. Any significant change to data collection or use should be reviewed with the school and, if needed,

incorporated into an updated contract or data privacy agreement to help the school maintain FERPA compliance and direct control. Guidance regarding contracts, data privacy agreements and privacy policies is contained in the Going Beyond Compliance section.

Parent Access

While parents have the right to access and seek to correct information in an education record, FERPA does not require service providers to respond directly to parent requests for access or correction. Typically, parents exercise their FERPA rights by approaching the education institution that maintains their child's education record. Service providers should work with education institutions to establish processes whereby schools can make requests on behalf of parents to access, correct, or delete student data. Note that some states may have additional laws that govern parental access.

No Waiver of Rights

There is *No Waiver of Rights* exception within FERPA. Schools cannot ask parents to waive their rights and cannot enter into contracts, terms of service, and other common legal agreements that waive rights granted by FERPA. If a service provider receives information from education records that is subject to FERPA, it must comply with the requirements of the law regardless of contractual waivers.

Enforcement

Although FERPA technically does not apply to service providers, they must understand their responsibilities and limitations as processors of student data. If the Department of Education discovers a FERPA violation involving a service provider, the provider can be prohibited from doing business with districts in which the violation occurred for up to five years. School districts found to be in violation of FERPA could also lose all of their federal funding.

Protection of Pupil Rights Amendment (PPRA)

The **Protection of Pupil Rights Amendment** grants parents notice and opt-out rights when schools ask students to provide certain categories of information. It also provides protections from the use of student information for the purpose of marketing or for selling that information.

PPRA allows parents to prevent the collection of their children's data when schools administer surveys as part of federally funded activities. If a school survey asks students about certain sensitive topics, such as religious beliefs, family income, political background, or social behaviors, PPRA requires schools to notify parents and allow them to opt their children out of participating. In addition, schools must notify the parents of students who will participate in activities involving the collection, disclosure, or use of personal information for marketing purposes, and must also give parents the opportunity to opt out of those activities. The notice, opt-out, and other requirements of PPRA do not apply when schools use students' personal information from surveys for the exclusive purpose of developing, evaluating, or providing educational products or services.

While PPRA's requirements apply only to schools, service providers should know that if they give surveys or utilize marketing tools as part of a service that a school pays for or directs, PPRA may apply. Similar to the rules of FERPA, if an investigation finds that PPRA has been violated, schools may lose federal funding or be ordered to cease doing business with the provider involved in the violation.

National School Lunch Act (NSLA)

The **National School Lunch Program (NSLP)** is administered by the U.S. Department of Agriculture and authorized by the **National School Lunch Act (NSLA)**. A student's free or reduced-price lunch (FRL) status is governed by NSLA and is not considered part of their education record. The NSLA has different confidentiality and disclosure requirements than FERPA and strictly prohibits the disclosure of a student's FRL status unless direct parent consent is provided. This consist must be provided to the district annually and detail who will have access to the status and how it will be used. According to Section 9 (b)(6)(C) of the NSLA, improper disclosure may result in a fine of up to $1000 or imprisonment of up to one year, or both. Improper disclosure includes publishing, divulging, disclosing, or making known in any manner or extent not authorized by Federal law, any eligibility information. Service providers should give special consideration to any collection or use of student FRL information as they may unintentionally violate the NSLA.

Below is information from the Eligibility Manual for School Meals Determining and Verifying Eligibility regarding disclosure requirements (page 86)

Disclosure Requirements

The NSLA allows persons directly connected with the administration or enforcement of certain programs or activities to have access to children's eligibility information. The following table, Disclosure, shows the circumstances for disclosing eligibility information. LEAs with concerns or questions about disclosing children's eligibility information should contact their State agency for further guidance.

Disclosure		
Recipient of Information	**What May Be Disclosed**	**Requirements**
Programs under the NSLA or CNA	*All eligibility information*	*Prior notice and consent not required*
Federal, State, or local means tested nutrition programs with eligibility standards comparable to the NSLP	*Eligibility status only*	*Prior notice and consent not required*
Federal education programs	*Eligibility status only*	*Prior notice and consent not required*
State education programs administered by a State agency or LEA	*Eligibility status only*	*Prior notice and consent not required*
Local education programs	*No eligibility information, unless parental or guardian consent is obtained*	*Parental or guardian consent*

Title II of the Americans with Disabilities Act (ADA)

On April 24, 2024, updated regulations under Title II of the Americans with Disabilities Act (ADA) established specific requirements, WCAG 2.1 Level AA, to ensure that web content and mobile applications are accessible to individuals with disabilities. The rule sets a defined technical standard that state and local governments—including public schools—must follow. Under these requirements, schools must ensure that digital learning resources delivered through websites or mobile apps are accessible, appropriate for, and usable by students with disabilities. CAST provides guidance on Universal Design for Learning and additional information about the updated Title II ruling and its implications for schools and service providers.

Health Insurance Portability and Accountability Act (HIPAA)

The **Health Insurance Portability and Accountability Act** protects the privacy and security of individually identifiable health information.

HIPAA generally does not apply to student data as the law protects health information held by a "covered entity," which typically does not include elementary and secondary schools. In fact, the HIPAA rule specifically says it does not cover information that is subject to FERPA. Personally identifiable information, including health information maintained by a school is typically considered part of the education record.

However, an increasing number of schools contract with service providers to support health services in schools, such as billing medical insurance for care. In these cases, any health information that is not subject to FERPA ***may*** fall under HIPAA. For example, information collected by a local health organization that comes to school to provide vaccinations or screenings for diseases would be covered under HIPAA. For a detailed examination of how HIPAA functions in schools, see the Department of Health and Human Services and Department of Education's joint guidance.

State Laws and Student Data Privacy

Online service providers need to know state-level student privacy laws and new laws on general data privacy, because both affect how they may use student data.

A majority of states have passed student privacy laws with requirements that apply directly to online service providers. In addition to establishing laws focused on student data, some states have created privacy and security laws with implications for education, such as data breach laws in all 50 states. Some states go as far as imposing specific security requirements on schools or edtech providers by incorporating the National Institute of Standards and Technology (NIST) Cybersecurity Framework or the HIPAA Technical Safeguards into legislation. Moreover, over 20% of states recognize a constitutional right to privacy. One significant challenge for companies is that state laws often define terms (such as PII) inconsistently and have unique requirements. The Data Quality Campaign provides annual information on state laws as well as other privacy tools and resources.

What Are Common State Level Approaches to Regulating Student Data?

States have typically approached the regulation of student data use in one of three ways. The first is by regulating schools (LEAs) and state-level education agencies (SEAs). For example, Oklahoma's 2013

Student Data Accessibility, Transparency, and Accountability Act (Student DATA Act) addressed permissible state-level collection, security, access, and uses of student data. Bills following the Oklahoma model have limited data collection and use and defined how holders of student data, including online service providers, can collect, safeguard, use, and grant access to data.

The second approach has been to directly regulate online service providers that collect and use student data. For instance, California's Student Online Personal Information Protection Act (SOPIPA) prevents online service providers from using student data for commercial purposes, while allowing specific beneficial uses such as personalized learning. California supplemented SOPIPA by enacting AB 1584, a law that explicitly allows districts and schools to contract with third parties in order to manage, store, access, and use information in students' education records. An enforcement provision, AB 375, was also added to give the California Attorney General additional authority to fine companies that violate SOPIPA and AB 1584. This law has become a model for the regulation of edtech service providers' use of student data. More than 20 states have since adopted similar laws.

The third approach combines the first two models. For instance, to regulate its state longitudinal data system, Georgia chose to follow Oklahoma's lead in addressing three core issues regarding state education entities: what data is collected, how student data can be used securely and ethically, and who can access student data. Combined with SOPIPA-like regulation of third parties, this approach has allowed innovative uses of student data while establishing meaningful privacy protections for students. Similarly, Utah has taken a modified hybrid approach by regulating districts, the state education agency, and service providers.

Since 2015, state legislation has tended to regulate data use rather than collection, and to focus laws on specific privacy topics such as data deletion, data misuse, biometric data, and breach notification. Unfortunately, no state or federal law exists that allows a service provider's compliance to also meet the requirements of all other student privacy laws across the country. Providers must be aware of each state's laws and adapt their policies and practices accordingly.

Do General State Privacy Laws Address Student Data?

As of late 2025, only California and New Jersey's state-level general privacy laws are written broadly enough to apply in the school context. It is important to be aware of the possible impact of these general privacy laws, as they may cover schools or create unintended consequences regarding education data. In California, the CPRA exempts businesses working on behalf of a local educational agency (LEA) from complying with a deletion request for a student's grades, educational test scores, and educational test results.

This framework introduces two fundamental challenges: First, the inclusion of three categories of student data—grades, test scores, and test results—in the CPRA implies all other student data held by a business on behalf of an LEA is subject to a deletion request, which could be interpreted as requiring the deletion of student data that is not addressed by the listed categories. Additionally, the provision's description of student data as data "that the business holds on behalf of a local educational agency," implies companies that provide services to schools are considered "businesses" subject to the law.

Going Beyond Compliance: Making Student Privacy a Priority

Online service providers play an important role in supporting school use and management of student data. For edtech service providers committed to protecting student data and establishing strong privacy practices, legal compliance is only the starting point. Going beyond the minimum requirements means understanding school districts' privacy expectations and actively collaborating with them to build trust and ensure data protection.

What is the Online Service Providers' Role in Protecting Student Privacy?

High-profile data breaches at major technology companies, along with ongoing data security incidents in both K–12 and higher education, have heightened public sensitivity to privacy risks. In education, these concerns are amplified by a shared understanding among stakeholders that children warrant heightened privacy protections. As a result, fears about inappropriate data use or disclosure now pose serious risks for edtech providers—both in terms of legal compliance and public perception.

An online service provider's approach to privacy can significantly influence its success. As schools adopt more technology, one of the greatest risks to edtech providers is public perception—particularly the risk that parents or districts may view a provider as irresponsible with student data. This perception, often fueled by a lack of trust and transparent communication, has impacted companies' reputations and long-term viability. The collapse of the education nonprofit inBloom in 2014, following widespread public backlash over its data-sharing practices, remains a pivotal example of how public trust can shape the edtech landscape. More recent data breaches involving EdTech service providers have reinforced expectations for strong data security, transparent practices, and accountability in vendor relationships—underscoring the continued importance of responsible data governance in K–12 education.

As part of responsible student data governance, many school districts now expect online service providers to adopt privacy practices aligned with a core set of commitments. These commonly include collecting and using student personal information only for authorized educational purposes, prohibiting its sale or use for targeted advertising, supporting access and correction rights, maintaining robust data security programs, and ensuring that subcontractors follow equivalent standards. These expectations are often embedded in contracts, privacy policies, and direct negotiations with educational institutions.

To meet legal obligations and earn the trust of schools, parents, and students, online service providers must recognize the unique sensitivity of student data and act responsibly. Successful providers often distinguish themselves by proactively communicating their privacy practices and demonstrating a commitment to protecting student information. To assist providers, the Software & Information Industry Association has developed a series of resources for educational companies and third-party companies.

Leveraging Contracts and Data Privacy Agreements

School districts often have formal policies that govern contract language, approval and execution. These policies–which apply to all contracts, even those for free services–typically establish procedures that ensure the district aligns with their data governance and security requirements, and designate specific individuals authorized to enter into contracts on the district's behalf.

Most districts limit contract-signing authority to a small number of individuals, such as the school board president, superintendent, or another designated administrator. To ensure the contract is valid and enforceable, providers must confirm that the individual signing the agreement has the legal authority to do so. Accepting a contract signed by an unauthorized school employee can lead to delays, compliance issues, or unenforceable terms. This challenge is especially relevant for online service providers that use "click wrap" agreements accepted by individual educators without district-level approval. Providers should establish a clear internal review process to verify that all agreements are executed in accordance with district policy and applicable legal requirements.

To streamline contracting and promote consistency, districts across the country—often with support from state education agencies or national organizations—have adopted model contracts and standardized data privacy agreements (DPAs). Two widely referenced resources include the Model Terms of Service published by the U.S. Department of Education's Privacy Technical Assistance Center (PTAC) and the National Data Privacy Agreement (NDPA) developed by the Student Data Privacy Consortium (SDPC). These frameworks offer schools legally vetted language and practical standards for ensuring the school's compliance with FERPA and state-level student privacy laws.

While model contracts help reduce administrative burden—especially for districts managing hundreds of vendor agreements—they are not always one-size-fits-all. However, there are common contract provisions including clauses addressing data breach notification and liability, cybersecurity insurance, survivability of obligations, and governing law. Terms related to data handling, direct control, and data security are often found in both the privacy policy and the DPA.

Service providers should review model language carefully and work collaboratively with districts to negotiate or revise terms that do not align with their services, while still upholding strong privacy and security commitments. It is essential to ensure that the contract signed by the district aligns with any referenced DPA. Inconsistencies between the main contract and the DPA can create confusion around enforcement or interpretation. Additionally, during contract renewals, care should be taken to reaffirm the terms originally agreed upon—renewals should not default to the service provider's standard terms of service or privacy policy without explicit district review and approval.

Contract and ToS Red Flags: What to Avoid or Carefully Review

- Vague or Overly Broad Data Use Language: Language such as "we may use data for any lawful purpose" or "data may be used to improve our services" without clearly limiting that use to educational purposes does not allow for the use of the "School Officials" exception and prevents the school's ability to provide consent under COPPA
- Unilateral Right to Amend Terms: clauses allowing the service provider to change the terms of service or privacy policy without district approval undermines the district's ability to maintain direct control.
- Inadequate Data Breach Notification Terms: vague or missing breach notification timelines may result in non-compliance with FERPA and state disclosure requirements.
- Absence of Data Deletion or Retention Clauses: a lack of clear data lifecycle management poses compliance risks and increases the likelihood of unnecessary data exposure.

- ➢ Lack of Limitations on Subcontractors: service providers should require subcontractors to follow the same data privacy and security obligations as agreed upon in the contract.
- ➢ Ambiguous Ownership of Data: districts should retain ownership of student data and education records, and this should be explicitly stated in the agreement.
- ➢ Overly Broad Indemnification or Liability for Districts: contracts should fairly allocate liability, particularly for data breaches or misuse–state statutes may prevent districts from providing indemnification.
- ➢ Automatic Renewal with Standard Terms: renewal clauses should not revert to the provider's default terms of service or privacy policy without district approval.

Although managing multiple contracts across states and districts is complex, it has become a necessary part of ensuring school compliance with FERPA and applicable state privacy laws. Providers should adopt a contracting process that is scalable and manageable across multiple agreements. Regardless of variation, all contract terms should accurately reflect the provider's actual data practices. Importantly, any changes that affect a school's direct control over student data must be clearly communicated and contractually amended to maintain the school's FERPA compliance.

Elements to Consider When Writing a Privacy Policy

Privacy policies are one of the most visible ways online service providers communicate their data practices to schools, parents, and students. These policies—along with terms of service—outline how companies collect, use, share, and protect student data. Clear, accessible privacy policies are essential for building trust with education stakeholders and can serve as a competitive advantage for providers seeking to work with privacy-conscious districts.

As part of responsible student data governance, many school districts now expect online service providers to adopt and communicate privacy commitments that reflect both legal compliance and community expectations. These commitments should be explicitly reflected in a provider's privacy policy and must align with contractual obligations—especially any signed DPAs. Inconsistencies between a privacy policy and a district's DPA or service contract can introduce compliance risks and delay adoption. To mitigate this, providers are encouraged to maintain a dedicated privacy policy for educational users, distinct from general consumer-facing policies.

Common Commitments in Education-Focused Privacy Policies:

- ➢ Collect and use student personal information only for authorized educational purposes
- ➢ Do not sell student personal information
- ➢ Prohibit behavioral advertising or profiling based on student data
- ➢ Limit creation of student profiles to those needed for educational services
- ➢ Support access to and correction of student data
- ➢ Retain student data only as long as necessary for educational purposes
- ➢ Maintain strong data security measures

- ➢ Require vendors and successor entities to follow equivalent privacy protections
- ➢ Provide clear notice and obtain agreement before applying material changes to data practices

Writing effective privacy policies is both a legal and a communications challenge. Many companies struggle to strike the right balance between clarity and legal precision. Similarly, schools often face difficulty interpreting vague or discretionary policy language. PTAC's Model Terms of Service offers practical guidance including privacy policy language that supports better transparency.

PTAC Guidance for Best Practice Privacy Language

	Provision	GOOD! This is a Best Practice	WARNING! Provisions That Cannot or Should Not Be Included in TOS	Explanation
5	Data Collection	"Provider will only collect Data necessary to fulfill its duties as outlined in this Agreement."	*An absence of a data collection restriction (see left) could potentially allow vendors to collect a wide array of student information.* *Also watch for:* "If user gains access through a third-party website *(such as a social networking site)*, personal information associated with that site may be collected."	If the agreement relates to FERPA-protected data, a provision like the one represented in the "GOOD!" column may be necessary. Including a provision that limits data collection to only what is necessary to fulfill the agreement is a best practice. Providers may view user access to their services through a third-party social networking site as an exception to established rules limiting data collection.

	Provision	GOOD! This is a Best Practice	WARNING! Provisions That Cannot or Should Not Be Included in TOS	Explanation
8	Data Sharing	"Data cannot be shared with any additional parties without prior written consent of the User except as required by law." *Or* "The [School/District] understands that Provider will rely on one or more subcontractors to perform services under this Agreement. Provider agrees to share the names of these subcontractors with User upon request. All subcontractors and successor entities of Provider will be subject to the terms of this Agreement."	"Provider may share information with one or more subcontractors without notice to User." *Or* "Where feasible, Provider will require third-party vendors to comply with these Terms of Service."	While it is perfectly acceptable for providers to use subcontractors, schools/districts should be made aware of these arrangements and subcontractors should be bound by the limitations in the TOS.

Terms commonly addressed in both privacy policies and DPAs include data handling, breach notification, data security, direct control by the school, and third-party vendor responsibilities. Providers should ensure that any changes to these practices—particularly those affecting a school's FERPA compliance—are clearly communicated and contractually amended when necessary.
While maintaining separate, education-specific privacy policies may require additional effort, doing so demonstrates transparency, supports legal compliance, and reinforces a commitment to student privacy that is increasingly expected by school communities.

Establishing Data Security Standards

Establishing and maintaining strong data security standards is foundational to protecting student privacy and earning the trust of schools, families, and communities. Online service providers play a critical role in safeguarding sensitive information by embedding security protections throughout the design, development, implementation, and maintenance of their products and services. In today's risk environment, it is no longer sufficient to treat security as a one-time technical requirement—it must be a sustained and strategic commitment across the entire product lifecycle.

In addition to protecting student and child privacy, both the Family Educational Rights and Privacy Act (FERPA) and the Children's Online Privacy Protection Act (COPPA) require schools and service providers to implement data security measures. These laws mandate the use of "reasonable" administrative, technological, and physical safeguards to prevent unauthorized access to student information. Importantly, these requirements apply regardless of the specific technology or platform in use, reinforcing the need for consistent, well-documented security practices across all systems and tools.

Service providers should adopt a recognized cybersecurity framework—such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework or the Center for Internet Security (CIS) Controls—to guide their security programs. Aligning with a standard allows providers to implement

tested, widely accepted controls, and it enables clearer communication with districts about how those controls are being met. These frameworks help structure protections such as secure system configurations, data encryption, role-based access controls, detailed logging, and routine system audits. Configuring access based on user roles and protecting all sensitive data with encryption that meets or exceeds industry best practices are key expectations in the education sector.

Security must also be operationalized through regular internal reviews and third-party assessments, which help identify vulnerabilities and verify the effectiveness of security controls. Providers should be prepared to share documentation that demonstrates how their systems meet defined standards and what processes are in place to monitor and adapt to new threats. Transparency and collaboration with districts are essential to ensuring digital learning environments remain secure, resilient, and aligned with legal and contractual obligations.

Equally important is the need for clear incident response and breach notification protocols. Providers should define how they will communicate with school districts in the event of a security incident, including timelines for notification, roles and responsibilities, and steps for investigation and remediation. These protocols should be reflected in both internal security planning and external contracts.

Finally, providers should implement robust data lifecycle management practices. This includes the regular review, retention, and secure deletion of student data in accordance with contractual and legal requirements. Minimizing the retention of unnecessary data reduces the risk of accidental exposure or misuse and reinforces the principle of data minimization embedded in many privacy laws.

Key Security Practices for Online Service Providers:

- ➢ Align with a recognized cybersecurity framework (e.g., NIST, CIS)
- ➢ Use encryption standards that meet or exceed industry best practices
- ➢ Configure access based on user roles and responsibilities
- ➢ Conduct regular internal and third-party security assessments
- ➢ Maintain detailed activity logging and secure data transfer protocols
- ➢ Establish clear breach notification and incident response protocols
- ➢ Implement data lifecycle management (review, retention, secure deletion)

By adopting a recognized standard, aligning practices across the product lifecycle, and communicating those practices clearly to education partners, online service providers can demonstrate their commitment to student data protection and meet the evolving expectations of the K–12 privacy landscape.

Navigating Student Privacy with AI and Emerging Technology

As artificial intelligence (AI) and other emerging technologies become more prevalent in educational tools, online service providers must carefully balance innovation with the core principles of student data privacy. These technologies often require or generate large volumes of data, raising new challenges around transparency, oversight, and risk mitigation. While advanced systems offer the potential to personalize learning, detect early warning signs, or streamline administrative functions, they also introduce complexities that must be navigated thoughtfully and responsibly.

One of the core tensions when deploying AI or similar technologies in education is the tradeoff between data accuracy and data minimization. While large and detailed datasets may improve the performance of AI models, such practices can conflict with privacy principles that limit data collection to what is necessary for educational purposes. Providers must address this tension by adopting responsible development and deployment practices, clearly communicating how student data is collected, processed, and used, and minimizing the collection of non-essential information. These considerations are not exclusive to generative AI—other technologies such as biometric systems, predictive analytics, and adaptive learning platforms raise similar concerns.

Privacy risks in emerging technology environments must also be evaluated alongside security risks. Inadequate safeguards can lead to data overexposure, especially when schools cannot control which data fields are transmitted, or lack visibility into how third-party systems process or access student information. In some cases, privacy violations occur not due to malicious activity, but because school systems are unaware of the data pathways embedded in automated systems. Providers must implement strong technical controls—including access restrictions, secure configurations, and data segregation—while also supporting schools in maintaining oversight.

Transparency is essential. The "black box" nature of many AI and algorithmically-driven systems can make it difficult for school leaders to understand how information is used, what decisions are being made, and whether privacy or equity risks are being introduced. To build trust and ensure compliance, online service providers must clearly document data flows, provide meaningful descriptions of algorithmic functions, and share security practices—such as authentication protocols and breach response strategies. Schools must retain visibility into how student data is handled, even in systems that are automated or adaptive.

When a service provider introduces a new feature or tool that uses student data in a novel or significantly different way, it is critical to notify districts in advance. Any material change in the data collected or how data is used should be reviewed in collaboration with the school and, when necessary, reflected in an amended contract or data privacy agreement. This ensures the school can maintain its obligations under FERPA, particularly around direct control and informed consent. Unilateral implementation of new data-driven features—without district awareness or agreement—can create compliance gaps and erode trust.

To support responsible use of emerging technologies, online service providers should:

- ➢ Align privacy and security practices with existing frameworks and laws (e.g., FERPA, COPPA, state-specific statutes).
- ➢ Document and communicate how automated decision-making systems use student data.
- ➢ Engage school districts in early-stage conversations about data collection, retention, and oversight.
- ➢ Provide configurable privacy settings that allow schools to limit or disable features that collect non-essential data.
- ➢ Identify any changes to how data is used and amend contracts accordingly to ensure legal compliance.

➢ Establish policies and safeguards that anticipate emerging risks while preserving the educational value of the technology.

Ultimately, service providers must ensure that privacy, security, and transparency are embedded into the design and operation of AI and other advanced digital tools. Emerging technologies can enhance educational outcomes, but only if trust is maintained through clear governance, technical safeguards, and respectful data use practices.

FPFhas developed Vetting Generative AI Tools for Use in Schools, a checklist and accompanying policy brief to help schools vet generative AI tools for compliance with student privacy laws. The in-depth policy brief outlines the relevant laws and policies a school should consider, the unique compliance considerations of generative AI tools (including data collection, transparency and explainability, product improvement, and high-risk decision-making), and their most likely use cases (student, teacher, and institution-focused).

The EdTech Service Provider's Guide to Student Privacy with AI and Emerging Technologies

Online service providers play a critical role in protecting student data and maintaining trust with schools and families. By aligning practices with legal requirements and educational values, companies can demonstrate leadership in responsible data use and long-term commitment to student privacy.

Consider the following, which review and elaborate on key points discussed above:

- **Understand the importance and context of student privacy.** Student privacy is a deeply held public concern, particularly in K–12 settings where children are uniquely vulnerable. High-profile data breaches and privacy controversies have elevated expectations for transparency and accountability. Service providers must be attuned to both legal requirements and public perception as they design and implement student-facing tools.

- **Know and comply with federal and state laws.** While FERPA applies directly to educational institutions, service providers acting as "school officials" must help ensure that their practices enable schools to meet their legal obligations. If a provider's actions cause a school to violate FERPA, the U.S. Department of Education may prohibit the provider from contracting with districts for up to five years. In addition, many state laws impose direct obligations and penalties on service providers for noncompliance. Because definitions and requirements—such as those related to personally identifiable information (PII)—can differ significantly across jurisdictions, providers must navigate a complex and evolving legal landscape with care and precision.

- **Honor FERPA rights and enable data access.** FERPA grants parents and eligible students the right to access and request corrections to education records. Providers should work with schools to establish processes that facilitate the exercise of these rights and ensure that data handling practices respect the school's obligations under FERPA.

- **Support core privacy commitments.** In addition to legal compliance, many districts now expect providers to align with core privacy commitments such as limiting data collection to authorized educational purposes, prohibiting the sale or targeted advertising of student information, supporting access and correction rights, and maintaining secure data environments. These commitments are often reflected in contracts, privacy policies, and district expectations.

- **Emphasize transparency when drafting privacy policies.** Effective privacy policies should clearly outline what data is collected, how it is used, and under what circumstances it may be shared. Providers should avoid vague language and ensure policies are written in accessible terms. Material changes to data practices must be communicated in advance, and any successor entities must uphold existing privacy commitments.

- **Implement data minimization and deletion practices.** Data should only be retained for as long as necessary to fulfill educational purposes or comply with legal obligations. Providers should

establish data lifecycle management protocols, including secure deletion processes for inactive accounts and routine audits to eliminate unneeded information.

- **Ensure the security of student data.** Security is a foundational element of privacy. Providers should align their practices with established frameworks such as the NIST Cybersecurity Framework or CIS Controls. FERPA and COPPA also require "reasonable" security measures regardless of technology used. Encryption, access controls, and incident response planning are essential components of a sound security program.

- **Ensure that subcontractors also follow best practices.** When subcontractors access student data, they must be held to the same privacy and security standards. Contracts should specify permitted uses, prohibit unauthorized redisclosure, and require adherence to all applicable laws. Providers are responsible for ensuring subcontractor practices do not undermine their own privacy commitments.

- **Plan for responsible use of emerging technologies.** As AI and other emerging technologies become integrated into educational tools, service providers must prioritize transparency, data minimization, and privacy-by-design principles. Providers should document data flows, clarify how automated features use student information, and ensure schools retain oversight. Any new or substantially modified features that change data use should prompt review and possible contract updates to support continued FERPA compliance.

The EdTech Service Provider's Student Privacy Checklist

Legal and Policy Compliance

- ☐ Understand and comply with all applicable federal and state student privacy laws. Someone within the organization maintains responsibility for evaluating contracts, product features, and data practices for legal alignment—this should not be a siloed or isolated responsibility.
- ☐ Ensure your practices as a "school official" support a school's ability to meet its legal obligations under FERPA.
- ☐ Establish a process for schools to request access, correction, and deletion of student PII in alignment with FERPA requirements.

Contracting Practices

- ☐ Confirm that only individuals authorized by district policy (e.g., superintendent or school board) sign contracts.
- ☐ Align contract terms with any referenced DPA and ensure renewals don't default to your company's standard terms without district approval.
- ☐ Review and adapt to model contract provisions such as those in the PTAC Model Terms of Service or the SDPC National Data Privacy Agreement.
- ☐ Address and document how your service handles data breaches, direct control, subcontractor responsibilities, data retention, and security standards.
- ☐ Establish internal processes to manage multiple district-specific contracts while maintaining consistency with actual data practices.

Privacy Policy and Transparency

- ☐ Publish a clear and accessible privacy policy that outlines data collection, use, sharing, retention, and security practices.
- ☐ Avoid vague terms—use definitive language to convey strong commitments (e.g., "will not sell," "must delete").
- ☐ Maintain education-specific privacy policies where applicable.
- ☐ Ensure your privacy policy aligns with your contracts and DPAs
- ☐ Collect, use, and retain only the data necessary for authorized educational purposes.
- ☐ Do not use student data for targeted advertising or build personal profiles beyond educational use.

Data Security Standards

- ☐ Adopt a recognized cybersecurity framework (e.g., NIST CSF, CIS Controls) to guide your security practices.
- ☐ Use strong encryption for data in transit and at rest; apply role-based access controls and secure configurations.
- ☐ Conduct regular security assessments and audits—both internal and third-party—and address any

vulnerabilities promptly.

- ☐ Maintain a documented incident response and breach notification plan that aligns with district and legal expectations.
- ☐ Implement data lifecycle policies that minimize data retention and support secure deletion practices.

Product Design & Emerging Technology

- ☐ Inform the school and amend agreements if you introduce new features or data uses that alter how data is collected, used, or disclosed.
- ☐ Embed privacy-by-design principles across the product lifecycle, from development to decommissioning.
- ☐ Transparently explain how AI and other automated features use student data—avoid "black box" designs that obscure decision-making.
- ☐ Minimize data used in AI systems and ensure districts understand and can audit data flows and risk mitigation practices.

Conclusion

The edtech industry is teeming with new innovations, many of which can improve the lives of students, parents, and educators. Schools value edtech providers for their creativity, talent, and foresight in providing meaningful educational services.

Despite the rapid legislative activity addressing student privacy, the speed of innovation can outpace regulation. To sufficiently protect student privacy, providers must ensure that products and services comply with applicable laws, and should go beyond compliance and implement applicable best practices. Following best practices to ensure strong security and privacy will build goodwill with education communities and leaders. When providers proactively address the concerns of parents, students, and administrators, they can also minimize business risks such as fines, investigations, and diminished trust. Prioritizing student privacy is a win for students, schools, and service providers.