

CoSN Student Data Privacy Initiative

Privacy Questions for Service Providers

When it comes to protecting student data privacy, one of the biggest challenges facing school district technology leaders is knowing how to ensure that student data privacy remains protected when it's shared with service providers, including enterprise level technology providers, providers of classroom technologies, community service organizations, and more.

The first step in accomplishing this goal is to understand each provider's privacy and security practices. Of course, that's sometimes easier said than done, but for privacy, it starts with reading the applicable privacy policy and terms of use. This is a foundational step to learning about the fundamental data privacy practices for each provider that will be collecting or otherwise accessing student personal information.

As part of that work, you may also need to look beyond the privacy policy and terms of use in order to gather additional details until you have enough information to be able to make an informed decision about whether or not a particular provider's privacy practices are sufficient to meet your district's requirements. Only *after* you have made a determination that a provider's privacy practices are adequate is it appropriate to move to the next step of executing a contract, inclusive of a data protection agreement. The diligence you conduct in advance of executing a data protection agreement is the "verify" part of the phrase, "Trust, but verify."

Privacy Questions to Consider:

Here are just a few of the basic questions to consider of any company, organization, or other service provider with whom you might need to share student personal information, as well as some of the reasons why these questions matter. *This is not all-inclusive but is intended as a tool to help you in getting started.* As you review this list, consider what other questions might be important in your district, and what else you might want to know to further your understanding of a provider's privacy practices.

Question	Why This Matters
What is the service being provided?	The district needs to assess whether the service provider would qualify as a “school official” under FERPA, or to determine under what other authority it is permitted to disclosure student personal information, such as with prior, written parent consent for the disclosure, or via another exception to parent consent articulated in FERPA that is applicable and appropriate to the situation.
What personal information will be collected from or about students, teachers, and administrators?	<p>The district needs to know what personal information is expected to be shared in order to evaluate the sensitivity of that data, whether the district is comfortable sharing that data based on the sensitivity, to be able to articulate the required protections on that data based on the sensitivity, and to maintain a record of the disclosure.</p> <p>Remember that even if students are accessing a product or service without creating an account, personal information requiring protection may be collected (and an education record may be created).</p>
Of the personal information that will be collected, what is minimally required in order to provide the services?	Some personal information may be needed only if certain features or services are enabled. Where there is discretion, the district should be aware so that it can ensure it is sharing only what is minimally required for the expected services.
Who will the personal information be collected from?	If the personal information will be collected directly from students, it may trigger additional legal considerations that need to be addressed, such as those related to the Children’s Online Privacy Protection Act, the Protection of Pupil Rights Amendment, or other applicable laws.
How will the personal information be collected?	Personal information may be collected in a variety of ways, including directly from the individual who actively enters the data, passively collected via different tracking technologies, uploaded to the provider directly from your district systems, or sent to the provider via a third party data sharing service. Regardless of the method, the district should verify that it is appropriate, permissible, and secure.
What will the personal information be used for?	Remember that under the school official exception in FERPA, student personal information may only be used for the district’s legitimate educational interests, similar to the permitted K12 purpose articulated in many state student data privacy laws.
What third parties operating in connection with the product or service will be receiving personal information, and for what purpose?	Understanding the third party footprint is important to verifying that the personal information will be used only for the purposes articulated by the provider and agreed to by your district.

<p>Is the product only permitted to be used by individuals of a certain age?</p>	<p>If the provider sets age limitations on its products (such as by prohibiting use by young students), it often means that the provider is not equipped for, or the product is not designed to meet the legal requirements for collecting personal information of individuals outside of those age limitations. It may also mean that the product is not appropriate for other ages.</p> <p>The district must know and be able to abide by these restrictions.</p>
<p>How will the company support your district's compliance with FERPA as it relates to your use of the product or service?</p>	<p>Remember that a company can't "comply with FERPA," as FERPA applies to educational institutions. However, if you have designated the provider as a "school official," they can (and must) ensure that they remain under your direct control with respect to their use and maintenance of student personal information.</p> <p>Providers should also be able to support you in other obligations that you have with respect to your compliance with FERPA, such as those related to responding to rights requests and more as applicable to the product or service being provided.</p>
<p>How will the provider respond to rights requests?</p>	<p>The district should understand the process that the provider has in place for responding to rights requests, including as applicable, that requests from students or parents will be forwarded to the district, whether the provider offers "self-serve" functionality to the district access, correct, and delete personal information or how the district should contact the provider with requests, and the expected timeliness of a response.</p>
<p>How does the provider intend to notify you in the event of a security incident resulting in unauthorized access to or release of your district's personal information?</p>	<p>At a minimum, you should be assured that the provider will notify their contact of record at the district promptly and without undue delay, in accordance with all legal requirements. (You may also want to consider imposing a reasonable time frame to articulate what the district intends by "promptly and without undue delay.")</p>
<p>Will the provider notify you of changes to their privacy policy? Will they notify you and request your consent for material changes to their privacy policy?</p>	<p>Cosmetic changes may not require consent, however material changes to a privacy policy would include changes in how personal information that has been previously collected is used, as well as any lessening of previously articulated protections, so that should be done only with your consent. Also remember that once you designate a provider to be a "school official," you must maintain "direct control" of the student personal information in their care.</p>

<p>When will the personal information be securely destroyed?</p>	<p>Typically, personal information should be kept only for as long as is necessary for the purpose for which it was provided. In addition, the provider may have the rights to access student personal information only for the duration of the contract. When the contract has no termination date, the provider may have set a policy to securely destroy personal information after the services have not been used for a certain period of time, or it may be up to the district to notify the provider when the personal information may be deleted.</p> <p>Whatever the arrangement, the district must know the time frame in order to be able to consider whether the district is in agreement with the retention period, given the services being provided.</p>
--	---

You may find these answers in a product or service provider’s privacy policy and terms of use, or you may need to approach the provider directly to get the answers you seek. The important thing is to ensure that you have the answers you need as part of your district’s privacy vetting process to be able to decide whether or not an organization is worthy of access to your students’ personal information at a level that would lead your district to consider executing a contract and data protection agreement.

Additional Resources:

[CoSN Student Data Privacy Toolkit Part 1: Student Data Privacy Fundamentals](#)

[CoSN Student Data Privacy Toolkit Part 2: Partnering With Service Providers](#)

[Building a Trusted Learning Environment: Understanding the Business Practice](#)

CoSN is vendor neutral and does not endorse products or services. Any mention of a specific solution is for contextual purposes.

About CoSN - The Consortium for School Networking

CoSN, the world-class professional association for K-12 EdTech leaders, stands at the forefront of education innovation. We are driven by a mission to equip current and aspiring K-12 education technology leaders, their teams, and school districts with the community, knowledge, and professional development they need to cultivate engaging learning environments. Our vision is rooted in a future where every learner reaches their unique potential, guided by our community. CoSN represents over 13 million students and continues to grow as a powerful and influential voice in K-12 education.

CoSN also provides opportunities for companies that support the K-12 EdTech community to participate as corporate members.

[CC BY-NC-ND](#)

