CoSN
LEADING EDUCATION INNOVATION

CoSN Student Data Privacy Toolkit

PART 3

Transparency and Trust

CoSN
LEADING EDUCATION INNOVATION

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

Introduction

Building and maintaining a student data privacy program can be an exceptionally challenging, but very necessary part of any School Systems' operations. CoSN's Student Data Privacy Toolkit is intended to support School Systems in these efforts, helping to guide School System leaders down the pathway from getting started with the work to engaging in a cycle of continuous improvement over time.

Protecting student data privacy is part of the responsibility of care that School Systems have for their students. An important part of the work includes ensuring that parents and other community members understand the School System's data privacy program, including how the School System manages its Student Data privacy responsibilities within the institution and when working with technology Providers.

Parents and other community members are often anxious about Student Data privacy matters, and those concerns can be eased in part by providing community members with clear information about the steps the School System takes to protect Student Data privacy. Showcasing a School System's competence around these matters helps to build community confidence.

Of course, earning the confidence and trust of the community takes time and dedicated effort, but the rewards of being able to partner with an informed and supportive community are well worth it. Leveraging a multi-faceted approach to the communications about your Student Data privacy program can help to ensure that all community members are able to access your materials in the way that works best for them.

In this section three of the CoSN Student Data Privacy Toolkit, we'll discuss some of the information School Systems should share with parents in order to not only comply with key student data privacy laws, but also to reach beyond the laws and provide parents with insights into your Student Data privacy program. These insights help to foster the understanding that your School System is making best efforts in the important work of protecting the students in your care.

If you've not yet reviewed sections one and two of the CoSN Student Data Privacy Toolkit, we encourage you to do so before reviewing this part. Section one addresses "Student Data Privacy Fundamentals," covering the basics of key student data privacy laws. Section two focuses on "Partnering with Providers," providing guidance for School Systems on approaches to assessing technology providers in light of the student data privacy law requirements.

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.

Communicating with Parents: Legal Requirements

As discussed in part one of the CoSN Student Data Privacy Toolkit: Student Data Privacy Fundamentals, there is a complex ecosystem of federal and state laws that support protection of Student Data privacy. Within these laws are a variety of requirements to provide parents and eligible students with information to help them make informed decisions about the student's privacy.

The chart below outlines select requirements.

Family Educational Rights and Privacy Act (FERPA)
School Systems covered by FERPA must: 1. Provide parents and eligible students with an annual notice advising of their rights, including their rights to: • inspect and review the student's education record; • seek amendment of the student's education record that the parent or eligible student believes to be inaccurate, misleading, or in violation of the student's personally identifiable information in the student's education records; • file a complaint with the US Department of Education (ED) about alleged failures by the School System to comply with FERPA requirements; • consent to disclosures of personally identifiable information in the education record, except to the extent that an exception to such consent in FERPA applies. The notice must include the procedures for: • exercising the right to inspect and review records; • requesting amendment of education records; AND • if the School System discloses education records under the FERPA "School Officials" exception, it must also provide the specific criteria used for determining who constitutes a school official and what constitutes a legitimate educational interest. School Systems must take care to effectively notify parents or eligible students who are disabled, and parents of elementary and secondary school students whose primary home language is other than English.

Continues.

Family Educational Rights and Privacy Act (FERPA)
2. Provide public notice to parents and eligible students of: • the types of personally identifiable information that the School System has designated as directory information • a parent's or eligible student's right to refuse to permit the School System to designate any of that information about the student as directory information; • the time period within which the parent or eligible student has to notify the School System in writing that they do not want any or all of those types of information about the student to be designated as directory information; The School System may specify that disclosure of directory information will be limited to specific parties, for specific purposes, or both. In doing so, of course, the School System must adhere to such attestations.
Protection of Pupil Rights Amendment (PPRA)
1. For surveys covered under PPRA and funded in whole or in part by ED, School Systems must notify parents and students who are 18 or older or are emancipated minors, at least annually, at the beginning of the school year of: • adoption or continued use of policies required under PPRA and activities covered by PPRA, including those activities that require the parent's or student's consent (notification must be provided within a reasonable time of any substantive change in those policies); • the opportunity for the parent or student to opt out of participating in a survey, assessment, or evaluation that reveals information related to any of the sensitive topics covered under PPRA; and • the date(s) when the covered activities may be conducted. Remember that parents also have the right to review any instructional materials used in connection with any survey that involves sensitive subject matter addressed by PPRA and those used as part of the educational curriculum.

Continues.

Children's Online Privacy Protection Act (COPPA)

COPPA applies to Providers that operate websites and online services directed to children under age 13, or those with actual knowledge that they are collecting personal information from children under age 13. COPPA does not apply to School Systems. However, in many cases, the Provider who must comply with COPPA may rely on the School System to authorize the Provider's collection of personal information from the covered students, or it may ask the School System to act as its intermediary in obtaining verifiable consent from parents prior to collecting personal information from the covered students.

In either case, the Provider is required to supply the School System a with notice of its information practices. Under COPPA, this notice should explain*:

- Where the parent's consent is required for the collection, use, or disclosure of personal information and that the Provider will not collect, use, or disclose any personal information from the child if the parent doesn't provide consent, and how a parent can provide verifiable consent prior to the collection, use, and disclosure of their child's personal information;
- Items of personal information that the Provider intends to collect from the child, or the potential opportunities for the disclosure of personal information, if the parent provides consent;
- A link to the Provider's online notice of its information practices.

**There are additional requirements for the notice if the technology provider had collected the parent's online contact information from the child in order to provide the notice, however that is typically not the case when the School System is acting on behalf of parents or as an intermediary for the technology provider.*

School Systems should work closely with their technology providers covered under COPPA to ensure that they understand the expectations related to providing the technology provider's COPPA notice to parents and obtaining their consent, as applicable.

There are, of course, a variety of other legally required notices under some of the above and other applicable laws that School Systems must provide to parents and eligible students. With all of that paperwork, it can be challenging to ensure that notice is effectively provided and understood. However, attention to those aspects is critical to ensuring that parents and eligible students are able to make informed decisions about privacy.

Assessing Your Communications Practices

How are you communicating about Student Data privacy with parents and students? Is it all captured in a flurry of paperwork sent home at the beginning of the school year? Do you use different media? Do you go beyond the legally required forms?

Parents and students need to know more than what's covered by the legal requirements. They need to know *how* your School System is complying with the laws. For School Systems, going beyond the legal communications requirements is a tremendous opportunity to start a positive, constructive conversation with your parents and students about Student Data privacy to build their confidence in your competence.

Here are some key questions to consider when it comes to building trust with parents and other community members about your Student Data privacy practices:

1. Are our legally required notices written in a way that parents and students can readily understand?
2. Are our teachers equipped to answer questions from parents about how the School System protects Student Data privacy and their role in the work?
3. Are our teachers equipped to explain to parents how classroom technologies are assessed for privacy and security practices prior to contracting?
4. What else can we share with parents and students to inform them about how we act to protect Student Data privacy?
5. How else can we help parents and students understand how we act to protect the security of the Student Data in our care?
6. How can our School System improve our communications with parents and students to help them understand how we consider privacy and security practices of our Providers?
7. Have we made it easy for parents and students to understand their rights and their choices regarding Student Data?
8. Have we provided parents and students with information to help them protect their own information privacy and security?
9. Have we taken steps to empower parents to take an active role in keeping their children safe on the internet?
10. Have we provided parents and students with a means to find out more about our School System's Student Data privacy and security programs?

These questions and more are critical to developing and improving a Student Data privacy communications program that will:

1. Help your parents and students understand how your School System acts to protect Student Data privacy;
2. Build trust and confidence in your Student Data privacy efforts, including as relates to your technology program; and
3. Build an ecosystem in which parents and students are partners with you in the work of protecting Student Data privacy.

All are important to help build a better understanding of your technology-enabled classroom within your parent community and reduce any fears or concerns about your collection, use, and sharing of Student Data.

> *It's critically important for parents and students to understand the steps you are taking to protect Student Data privacy. It reduces fear and concern, and builds the confidence needed to support your technology program, and weather any data issues that do arise. Show parents and students that they can trust you with Student Data to build a partnership with them around this important work.*

Getting Started

With the above questions in mind, here are some steps you can take to begin the work of improving and building out your communications regarding Student Data privacy.

1. Review your legal notices.

Take out that stack of paper you send home every year and review it. How easy is it to get through and to understand? Is it unnecessarily long? Is it written in legalese? If needed, start fresh with new or updated documents. Pay careful attention to the requirements and the ways they are communicated. While you're at it, try to make it visually appealing too. (Hint: don't cram as many words as you can fit onto the page.) This all helps to make it easier to read. Be sure that your legal counsel review it before you distribute it to parents, but work with them to keep it reader-friendly.

2. Explain why you collect Student Data.

Do parents and students know what Student Data your School System collects and why? If not, this is a good starting point for going beyond legally required notices. School Systems often collect a wide array of Student Data, and with good reason. Help parents and students understand why the data collection is necessary and how you make good use of the information to serve student needs. This simple step can go a long way to helping parents and students better understand your Student Data needs and the education system generally.

3. Demonstrate that your School System can be trusted.

Consider the question of why parents and students should have confidence in your ability to protect Student Data. This may seem obvious to School System technology leaders. After all, you spend much of your time engaged in the work of protecting Student Data privacy. However, parents and students are often unaware of the knowledge you've built around protecting the privacy and security of Student Data, the complexity of the work, or the ongoing investments you make attending to it.

Can you think of 5 things you would like parents and students to know about how your School System protects Student Data? One of them should be explaining how you assess privacy and security practices before contracting with and sharing Student Data with Providers. Communicating your "top 5" list will help build support for a trust-based relationship with your parents and student around your Student Data privacy program.

4. Share your expertise.

As a technology leader, you can help parents understand not only the work you do to protect Student Data, but steps they can take to protect their own information and that of their child at home. There is a world of free resources from credible sources available to leverage for this, including privacy tips, security guidance, internet safety advice, and more. You can be a leader to your community by regularly sharing resources covering these topics.

5. Reach your community where they are.

Remember that everyone has different preferences when it comes to how they like to learn best. When sharing information and guidance about your Student Data privacy program, or tips for parents and students to get empowered around their own privacy, try different formats and communication vehicles, and if you have a communications team, engage with them for guidance on what they've found to be most effective for community outreach.

ED's Student Privacy Policy Office (SPPO) and its Privacy Technical Assistance Center (PTAC) conducted a four-year review of a nationally representative sample of just over 1,500 School System websites to identify how School Systems are leveraging their websites to share information about Student Data privacy.

Their final report showed that School Systems are often not taking advantage of their own websites for privacy communications. Consider:

- **53%** of School Systems posted their annual FERPA notification
- **50%** posted their directory information policy;
- Only **28%** posted their PPRA policy.

Only 9% of websites had a navigation menu item that included a section indicating where to find information about data practices and privacy. Your website may very well be an untapped resource that you can leverage for greater transparency about Student Data privacy practices.

While not required, SPPO recommends as a transparency best practice that School Systems post their FERPA and PPRA privacy-related information on their websites so that it is easily available to parents, students, and the community.

Putting it Together: Building a Trusted Learning Environment

The CoSN Trusted Learning Environment (TLE) Seal is a mark of distinction for School Systems that have met a rigorous set of standards and demonstrated their commitment to protecting Student Data privacy. It was created by CoSN along with 28 School System leaders and lead partners AASA (the School Superintendents Association), ASBO (the Association of School Business Officials), and ASCD. It encompasses five practice areas: Leadership, Business, Security, Professional Development and Classroom. Together, these encompass requirements for an organizational approach to protecting Student Data privacy.

By earning the TLE Seal, School Systems signal to parents and communities that they are committed to protecting Student Data privacy and have taken concrete, measurable steps to do so in a way that is transparent to the community.

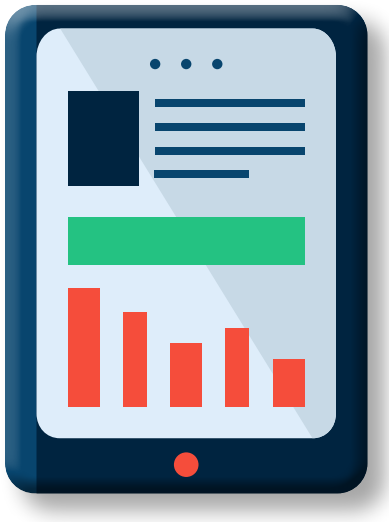
You can learn more about CoSN's Trusted Learning Environment Seal Program and meet the TLE Seal recipients here.

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. The CoSN Student Data Privacy Toolkits and additional resources are available at CoSN.org/Privacy and below.



Useful Links:

Training, Education and Communication

- CoSN Student Data Privacy Infographic
- CoSN: Building a Trusted Learning Environment with Parents
- PTAC Transparency Best Practices
- Data Quality Campaign Infographics
- Future of Privacy Forum Parents Guide to Student Data Privacy

Legal Notices

- FERPA Model Notification of Rights for Elementary & Secondary Schools
- Model Notification for Directory Information
- Model Notification for Directory Information En Espanol
- PPRA Model General Notification of Rights

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 specific policy 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.