

The Educator's
Guide To
**STUDENT
DATA PRIVACY**



by
Kerry Gallagher, Larry Magid, and Kobie Pruitt

ConnectSafely
Smart Socializing Starts Here™

 **FUTURE OF
PRIVACY
FORUM**

Technology tools and apps are making it possible for educators and students to collaborate, create, and share ideas more easily than ever. When schools use technology, students' data—including some personal information—is collected both by educators and often the companies that provide apps and online services. Educators use some of this data to inform their instructional practice and get to know their students better. It is just as essential for educators to protect their students as it is to help them learn.

This guide is meant to help teachers utilize technology in the classroom while protecting their students' privacy.

Why should classroom teachers care about student data privacy?

There are legal and ethical restrictions that impact districts, school, and teachers.

Traditionally, student data consisted of things like attendance, grades, discipline records, and health records. Access to that data used to be restricted to the administrator, guidance counselor, teacher, or other school official who needed it to serve the educational needs of the child. With the use of technology in schools, traditional data is now often shared with companies that provide Student Information Systems (SIS), Learning Management Systems (LMS), and many other technologies. Parents, students, and others have raised concerns about what information is being collected or shared, and what use those companies might make of that data.

Teachers should be aware of Family Educational Rights and Privacy Act (FERPA) and applicable state laws, along with their district or school policies regarding the use of educational products and services from ed tech vendors. (More on FERPA and other laws below)

New technologies—including personal computers, mobile devices, apps, websites, programs, and online services—are used in classrooms in ways that cause new data to be generated about individual students that never existed before including drafts and edits as they are recorded and showing the pacing and record of their performance through a math or reading program.

Communications between students and teachers, or students and other students—along with everything from last night’s math homework to the metadata of their online behavior while immersed in an app—is now created, collected, and often held by third party educational technology vendors.

Teachers are ethically obliged to follow and model good digital citizenship practices and behaviors with their students. This includes thinking carefully about the digital products and processes that are incorporated in any project or lesson design.



What constitutes student data?

Information that is tied to individual students is referred to as personally identifiable information, or PII, and is subject to additional restrictions in laws and regulations.

Student personal information includes any information about a student’s identity, academics, medical conditions, or anything else that is collected, stored, and communicated by schools or technology vendors on behalf of schools that is particular to that individual student. This includes a student’s name, address, names of parents or guardians, date of birth, grades, attendance, disciplinary records, eligibility for lunch programs, special needs, and other information necessary for basic administration and instruction. It also includes the data created or generated by the student or teacher in the use of technology—email accounts, online bulletin boards, work performed with an educational program or app, anything that is by or about the individual student in the educational setting. Some student personal information such as social security number, is highly sensitive and collection may be barred by state law.

What is an education record?

The federal law, FERPA protects educational records that contain information directly related to an individual student and which are maintained by an educational agency or institution or by a party acting for the agency or institution. However, new state student privacy laws protect all “student personal information” and data that is now collected and used via modern educational technology products and services.

What if I want to use an education app or tool and I don't know if my school/district has vetted it?

Be familiar with your school's policy or process for selecting new educational tools, if one exists.

If an app or service you want to use is not on the "approved" list, ask for it to be vetted and ask how long the vetting process takes. If the process is lengthy, you will want to redesign your lesson or project plan. Once the app is approved, you can certainly use it later. The list may also contain similar alternative apps you can use in the meantime.

If no such vetting process exists in your school, the checklist at the end of this guide can help you quickly evaluate whether your students' information will be protected.

Some tools have already been vetted

If your school or district has an approved list of ed tech products, services, websites, or apps, check that the service you use is included and ensure you are aware of any requirements or privacy options.

When schools and districts decide to adopt certain technology tools, they should evaluate those tools to ensure they meet data privacy requirements. Some examples include:

- Workflow and collaboration tools where students and teachers draft work together, give feedback, and communicate throughout the learning process.



- Learning Management Systems (LMS) where teachers post instructions, assignments, and links to resources for students and parents to access.
- Online gradebooks where teachers post grades and students and parents can access them using a username and password.
- Communication tools for emails or newsletters.

What about companies that provide online tools to schools?

Schools are allowed to rely on technology companies to provide products and services, but have the responsibility to ensure that those vendors have appropriate protections in place for student data. The school must ensure that it retains direct control over the information the company collects, uses, and maintains. Schools are responsible for seeing that companies working with the school directly only use student information for authorized educational purposes. These companies have access to this data under the “school official” exception, for the limited purpose of using student information for educational purposes only.

What should I do if a student suggests an unvetted education app to use for a project?

As a teacher, you cannot officially endorse use of an outside product, but you can explain to the student the considerations they should take into account, including recommending the student let their parents know too.

It's quite common for students to find education apps on their own to use for projects, and educators should encourage students to be creative and take their suggestions seriously. This is a teachable moment—a great opportunity to talk with the student about data privacy and review that digital citizenship curriculum.

Here are some examples of questions you could use to start the conversation with your student:

1. Did you have to make an account in order to start using that app? If so, did you have to provide personal information (email, name, age, etc.)?
2. Does the app require parental permission? Who has access to your email and other information now that you've created that account?
3. Does the app developer share your information with others? (It's in their privacy policy.)
4. Does the app collect additional information such as location or contacts?

In all likelihood, your student will not know the answers to some of these questions. That is OK, but it is important to explain to them that all of this information belongs to them. They should think about protecting it, and should be encouraged to discuss their choices at home with their parents as well.

What if my students and/or I want to use or recommend a technology tool that was not specifically designed for education?

If you, the teacher, want to recommend an app that was not specifically designed for education, checking with your administration, complying with applicable school policies, and using the checklist in this guide just as you would for an education-specific app is still a best practice.

It's a common issue because there are many "consumer apps," not designed for education that students may wish to use for learning or to help them with their homework and projects. These may include research tools, note taking apps, collaboration tools or apps that allow users to make videos, record audio or create other media such as cartoons, images, and so on.

However, commercial products not designed and marketed for schools may not have the privacy policies and practices in place to ensure the protection of user data to the standards of laws that protect student information. Therefore, if not prohibited by school policy, these products should be carefully evaluated to see if their use will put student data at undesirable risk.

If a student approaches you and asks to use an app for your assignment that you're not familiar with, it is a good idea to use the opportunity to talk to your student using the suggested questions above. Again, harness that teachable moment.

What are the federal and state laws that we need to follow?

FERPA – *Information in a student's education record is governed by the **Family Educational Rights and Privacy Act**, a federal law enacted in 1974 that guarantees that parents have access to their child's education record and restricts who can access and use student information.*

FERPA protects the access to and sharing of a student's education record, which is all information directly related to a particular student as part of his or her education. FERPA gives parents specific rights to their child's education records and when a child turns 18, the rights belong directly to him or her.

FERPA also permits schools to share information with another school system regarding a student's enrollment or transfer, specified officials for audit or evaluation purposes; appropriate parties in connection with financial aid to a student; organizations conducting certain studies for or on behalf of the school; and accrediting organizations. The "school official" exception allows schools to share information with parent volunteers, technology companies or other vendors, but only when used for educational purposes directed by the school. (See Sidebar.) Directory Information, another FERPA exception, is student data that a school may make public, for example a sports team roster, yearbook information or even data that can be provided to third parties, but parents must be given the opportunity to opt-out.

COPPA – The Children's Online Privacy Protection Act (COPPA) controls what information is collected from young children by companies operating websites, games, and mobile applications directed toward children under 13.

COPPA requires companies to have a clear privacy policy, provide direct notice to parents, and obtain parental consent before collecting information from children under 13. Teachers and other school officials are authorized to provide this consent on behalf of parents for use of an educational program, but only for use in the educational context. This means the company can only collect personal information from students for the specified educational purpose, and for no other commercial purpose. Some schools have policies that require school administrator approval before teachers can allow use of certain apps or services. When information is collected with the consent of a school official, the company may keep the information only as long as necessary to achieve the educational purposes.

PPRA – The Protection of Pupil Rights Amendment (PPRA) outlines restrictions for the process when students might be asked for information as part of federally funded surveys or evaluations.

For example, surveys might be used to better understand the effects on students of drug and alcohol use, or sexual conduct. They might also seek to understand the impact on students with family backgrounds that include violence, or variations in home life such as family makeup or income levels. In order to administer such surveys, schools must be able to show parents any of the survey materials used, and provide parents with choices for any surveys that deal with certain sensitive categories.

What resources are available to teachers to further understand and teach student privacy?

State laws vary greatly and you should be aware of your state's specific requirements.

If your school administration does not have information or training available on this topic, there are sites that can help you locate your particular state's law, and provide overall information on these questions. See the additional resources section below. What resources are available to teachers to further understand and teach student privacy?

- **ConnectSafely Educator's Guide to Social Media** explains how educators can use social media in the classroom without risking their professional reputation. [Connectsafely.org/eduguide](https://connectsafely.org/eduguide)
- **FERPAISHERPA** provides service providers, parents, school officials, and policymakers with easy access to materials and resources to help guide responsible uses of student's data. [FerpaSherpa.org](https://ferpaSherpa.org)
- **Student Privacy Pledge** is a list of twelve commitments K-12 school service providers agree to in order to safeguard student data privacy regarding the collection, maintenance, and use of student personal information. StudentPrivacyPledge.org
- **ConnectSafely, FPF, PTA Parent's Guide to Student Data Privacy** assists parents in understanding the laws that protect student data and helps parents understand their student's rights under the law. [FerpaSherpa.org/pdf/parents_guide.pdf](https://ferpaSherpa.org/pdf/parents_guide.pdf)
- **Department of Education PTAC** is a resource for education stakeholders to learn about data privacy, confidentiality, and security practices related to student-level longitudinal data systems and other uses of student data. ptac.ed.gov
- **CoSN Privacy Toolkit for School Leaders** provides school officials with 10 essential skills areas, outlining the responsibilities and knowledge needed to be an educational technology leader. cosn.org/focus-areas/leadership-vision/protecting-privacy
- **Data Quality Campaign** provides information on state laws annually, as well as other useful privacy review tools and resources. dataqualitycampaign.org/wp-content/uploads/2015/09/DQC-Student-Data-Laws-2015-Sept23.pdf

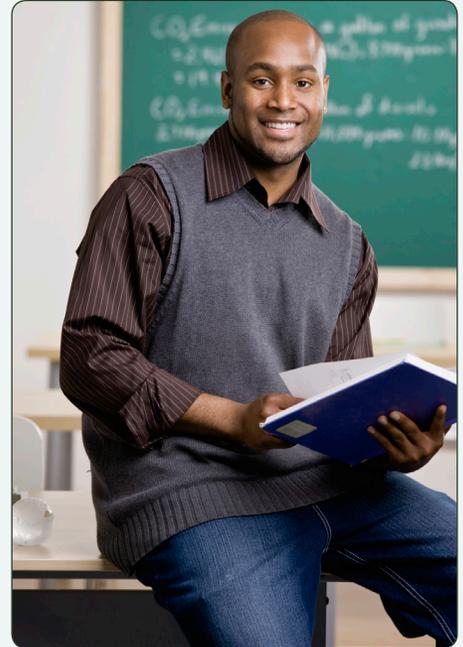


Closing thoughts for educators

We live in a period of constant change that affects everyone—families, government, business and, of course, education. It's an exciting time and, although rapid change can sometimes be hard to adjust to, it's a fact of life that's not going away.

For the most part, change is good, especially when it increases our productivity and improves outcomes and helps engage our students. But as we adopt new technologies, we must also think about how they affect the safety, security and privacy of all stakeholders—especially our students.

Sometimes it makes sense to pause, if even for a moment, to make sure we're doing all we can to protect our students. But it's also our responsibility as educators to embrace innovation and encourage our students and our colleagues to try new approaches and embrace new tools. It's a challenge, but it's not beyond our reach.



Some questions to help you quickly evaluate whether an app, website, product, or service will protect your students' information.

1. Does the product collect Personally Identifiable Information?
 - FERPA, the federal privacy law applies to “education records” only, but many state laws cover ALL student personal information.
2. Does the vendor commit not to further share student information other than as needed to provide the educational product or service? (Such as third party cloud storage, or a subcontractor the vendor works with under contract.) **The vendor should clearly promise never to sell data.**
3. Does the vendor create a profile of students, other than for the educational purposes specified? Vendors are not allowed to create a student profile for any reason outside of the authorized educational purpose.
4. When you cancel the account or delete the app, will the vendor delete all the student data that has been provided or created?
5. Does the product show advertisements to student users? Ads are allowed, but many states ban ads targeted based on data about students or behavioral ads that are based on tracking a student across the web.
 - TIP:** Look for a triangle i symbol (▶) which is an industry label indicating that a site allows behaviorally targeted advertising. **These are never acceptable for school use.** This would be particularly important when evaluating non-education-specific sites or services.
6. Does the vendor allow parents to access data it holds about students or enable schools to access data so the school can provide the data to parents in compliance with FERPA?
7. Does the vendor promise that it provides appropriate security for the data it collects?
 - TIP:** A particularly secure product will specify that it uses encryption when it stores or transmits student information. Encrypting the data adds a critical layer of protection for student information and indicates a higher level of security.
8. Does the vendor claim that it can change its privacy policy without notice at any time? This is a red flag—current FTC rules require that companies provide notice to users when their privacy policies change in a significant or “material” way, and get new consent for collection and use of their data.
9. Does the vendor say that if the company is sold, all bets are off? The policy should state that any sale or merger will require the new company to adhere to the same protections.
10. Do reviews or articles about the product or vendor raise any red flags that cause you concern?



About the authors

Kerry Gallagher (@KerryHawk02) is the Director of K-12 Education for ConnectSafely.org, in addition to her full-time role as Digital Learning Specialist at St. John's Prep in Danvers, Massachusetts. St. John's is a 1:1 iPad school serving 1500 students grades 6-12. Kerry taught middle and high school history in Bring Your Own Device public schools for 13 years. Kerry has a Juris Doctor from Massachusetts School of Law.

Larry Magid (@LarryMagid) is CEO and co-founder of ConnectSafely.org, a technology journalist with CBS News, San Jose Mercury News and other outlets and for 19 years a syndicated columnist for the Los Angeles Times. He has a Doctorate of Education from the University of Massachusetts at Amherst.

Kobie Pruitt (@FERPASherpa) serves as the Education Policy Manager at the Future of Privacy Forum (FPF). He operates as the program manager for FPF's work in student data privacy and ed tech. Kobie works with advocates, industry leaders and privacy experts to promote the growing need for education privacy standards. Prior to working at FPF, Kobie was a Legislative Assistant for Congresswoman Marcy Kaptur (OH-09). He handled an issue portfolio that included education, financial services and homeland security. He is a graduate of the University of Maryland Francis King Carey School of Law and the University of Pittsburgh, School of Business Administration.

