



## A Parents' Guide to **Student Data Privacy**



We live in an increasingly connected world where information flows between us and the organizations and companies we deal with every day. Historically that information was stored in filing cabinets but, today, most of it is stored on computers—sometimes accessible via the Internet.

Schools have always held a wide range of data about our children and families: Name, address, names of parents or guardians, date of birth, grades, attendance, disciplinary records, eligibility for lunch programs, special needs and the like are all necessary for basic administration and instruction. Teachers and school officials use this information for lots of reasons, including to assess how well students at a school are progressing, how effective teachers are at teaching, and how well your school performs compared to other schools. State departments of education collect data that is then aggregated (summarized) to help guide policy decisions and plan budgets.



Schools are also increasingly storing electronic data associated with “connected learning,” where online resources are used for instruction and evaluation. Online tools give students access to vast libraries of resources and allow them to collaborate with classmates or even peers around the world. Some of these online tools also give teachers and parents the ability to access and evaluate student work.

Whether information is on paper or online, the basic privacy rights for students and parents remain the

same. This guide will help you understand the laws that protect student data, as well as students' and parents' rights under the laws.

## **Who has access to information about your child?**

Information in your child's education record is governed by the Family Educational Rights and Privacy Act (FERPA), 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 applies to schools that receive federal funding, which are most public schools and some, but not all, private schools. FERPA protects the privacy 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, including the right to:

- Inspect and review your child's education record;
- Request corrections (or deletion) for anything that is inaccurate; and
- Consent, or deny, disclosure of some of your child's information in certain situations.

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. Schools may also disclose information to comply with a judicial order or subpoena; appropriate officials in cases of health and safety emergencies; and state and local authorities, within a juvenile justice system, pursuant to specific state law.



## **What is COPPA and when does it apply to information from students?**

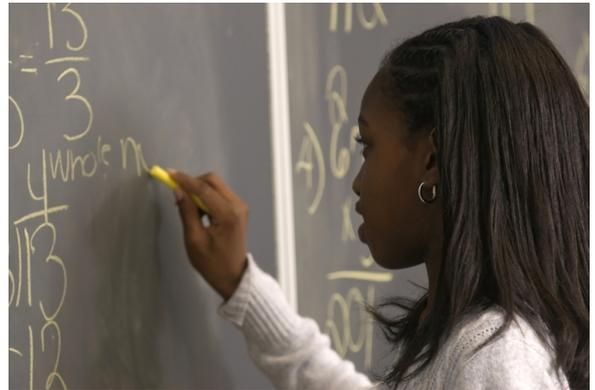
Children's Online Privacy Protect Act (COPPA), another important federal law, controls what information is collected from young children by companies operating websites, games, and mobile applications. It applies to online products directed toward children under 13 or when the company knows that a user is under 13.

COPPA requires that companies post a clear privacy policy on their site, and provide direct notice to parents, and obtain parental consent, before collecting information from children under 13. The law also provides parental access to the child's information and requires companies to delete it if asked. COPPA also requires that companies have the necessary security to protect the child's information.

Teachers and other school officials are also authorized to provide this consent on behalf of parents and can approve your child's use of an educational program. Importantly, the school's ability to consent on a parent's behalf is limited to the educational context—it applies only when the company collects 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.

## Are there other laws about student data?

The Protection of Pupil Rights Amendment (PPRA) outlines the information students might be asked 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 they have to get your consent in advance for any surveys that deal with certain sensitive categories such as political groups; psychological problems; sex behavior and attitudes; illegal behavior; close family relationships; relationships with lawyers, physicians, and ministers; or income (except to qualify for federal assistance such as reduced price meals). You may choose not to have your children participate in any of these surveys.

PPRA also provides parents with opt-out rights regarding certain types of marketing materials.



There are also restrictions on what information schools can share with the federal government, though it's important for parents to know that a provision in the Federal No Child Left Behind (NCLB) law and the National Defense Authorization require, with some exceptions, the disclosure of directory-type information to military recruiters, as well to recruiters from colleges and universities. However, if a parent opts-out of providing information to third parties, that opt-out also applies to military recruiters.

State laws and other federal laws may also protect student information. For example, the U.S. Department of Agriculture administers the National School Lunch Act (NSLA), which

has stricter privacy provisions than FERPA, and restricts who may see certain information about students who are eligible for free and reduced-price meals. And the U.S. Department of Health and Human Services enforces a law that requires strict confidentiality on information about student drug and alcohol prevention and treatment services.

It's important to note that these laws apply only to schools and not directly to the companies that schools hire to process and store student information. It's important that your school or school district have strong contracts in place with any vendors they use. And be aware that FERPA covers only education records, so some information collected by schools may not be covered. Some states have passed local laws filling in these gaps.

## **What about companies that provide online tools to schools?**

Schools are allowed to rely on technology companies to provide 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 uses and maintains, and companies working with the school directly may only use student information for the authorized educational purpose. The only exception is that companies may use the data internally to improve their programs or develop new products.

## **When do I have the choice to “opt out” of my child’s information being shared?**

Schools are allowed to publically share what is called “Directory Information” such as a student’s name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. It might also include email address, a photo, grade level, and participation in sports or other activities.

Schools are required to inform parents (and students 18 and over) about what information they have designated Directory Information and must allow a reasonable amount of time for parents to request that the school not disclose their child’s Directory Information.

The school may decide exactly how to provide the notice. For example, it can be in a special letter, a notice in a PTA bulletin, or a section of the student handbook. In response, parents wishing to opt-out must clearly request so in writing, within the stated timeframe, that their child’s information may not be released to third parties. (For how to gain access, make corrections, or request deletion of your child’s data, see sidebar.)



## Your child's data: How to gain access, make corrections, or request deletion

### FERPA access:

Under FERPA, you have the right to review (see) your child's education record at the school. Schools must provide this opportunity within 45 days of the request. However, schools are not required to provide copies of records unless it is impossible for you to review the records locally (for example, a long distance inquiry). If they have to make a copy, the schools may charge for the cost of the copies. Schools may not charge a fee to search for or to retrieve the records.

### Correction and deletion:

If you believe there is an error (inaccurate or misleading information) in your child's education record, you can ask to have the record corrected. You can also ask to have inaccurate information deleted. However, this right cannot be used to challenge grades, disciplinary rulings, or disability placements.

If the school does not agree to the change (or deletion), you have the right to a formal hearing. The school must have a process in place to allow an opportunity to challenge the school's decision. After the hearing, if the school still decides not to amend the record, you have the right to place a statement in the record stating your view. This statement must stay as a permanent part of the record.

If you believe that a school hasn't provided access properly, the Department of Education provides a process for you to formally complain about the school's performance. The complaint must be within 180 days. You must write down the following information on an official complaint form that is available by calling 1-202-260-3887.

- The date you were denied access;
- Name of the school official you asked;
- The response from the school official, if any; and
- The specific information (part of the student's record) that was requested.

### Mail the form to:

Family Policy Compliance Office  
U.S. Department of Education  
400 Maryland Avenue, SW  
Washington, DC 20202-8520

### COPPA concerns:

If you believe a company has misused your child's information, you can report this to the school and you can file a complaint with the federal Trade Commission. To file a complaint in English or Spanish, visit the FTC's online Complaint Assistant or call 1-877-FTC-HELP (1-877-382-4357) or register a complaint online at <http://www.ftc.gov/complaint>. Please note: the FTC does not resolve individual complaints, but the information is added to law enforcement databases to initiate or support ongoing investigations.

## Closing thoughts for parents

While laws apply to what schools and third parties can disclose about students, they do not apply to what students or their parents might disclose publicly, which means you and your child also have a responsibility to protect your child's privacy. What you or your child posts on social media, for example, could be used by others, including private companies and law enforcement in some cases, and is not protected by FERPA or any other federal law. Be certain you understand and use the privacy tools on any website or app that you or they use for school or at home to limit who can see your information (that includes having strong, secure and unique passwords; for tips, visit [ConnectSafely.org/passwords](http://ConnectSafely.org/passwords)), and be sure to never say anything online that you wouldn't want shared with others, including law enforcement, college recruiters and current or future employers.

