Student Privacy Primer

This primer explains the concepts of student data, including who uses the data and why they use it; data privacy in general; student data privacy; student data privacy risks and harms; how student data privacy relates to data ethics and data equity; key federal privacy laws; key district and school policies; and what it means to foster a culture of privacy. Each of these sections and a concluding section list additional resources to help education stakeholders learn more about student data privacy.

OCTOBER 2021

FUTURE OF PRIVACY FORUM

What Is Student Data?

Student data is student information that is collected and used in an educational context. This information has traditionally included data collected at school, but with increased use of online learning technologies, the educational context now includes data collected beyond the classroom, including from students' devices at home.

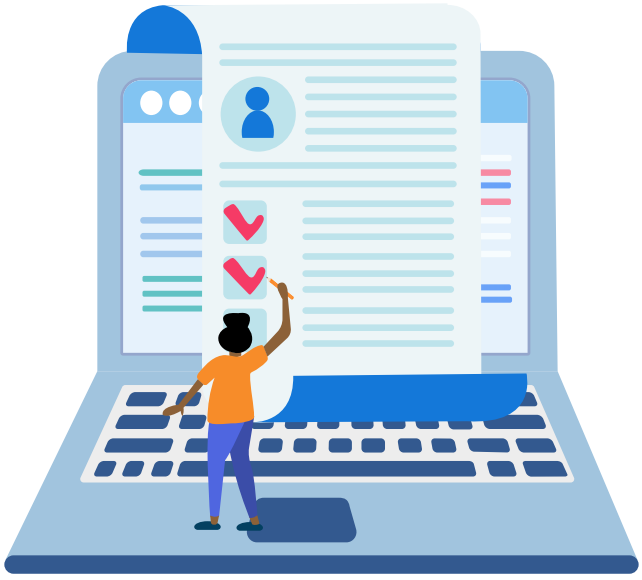
Examples of student data collected throughout a student's educational journey include

- Name, age, gender, race, ethnicity, socioeconomic status, and other demographic data that schools request or require when students register for school;
- Grades, test scores, attendance, discipline and health records, and college and career goals that schools track to help them follow a student's progression throughout their education career;
- Recorded observational data, which educators generate throughout the school day, about a student's behavior, motivation, or interests;
- Students' performance, time on task, and outcomes generated through homework, learning applications, and standardized tests; and
- Data that helps schools understand and assess students' needs, including internet and device access, transportation access, home circumstances, health needs, and food security.

Understanding the different types of student data enables better comprehension of the sensitivity and potential privacy risks associated with each type. This understanding, in turn, informs the data that schools and districts choose to collect, use, and share, as well as how the data is protected.

The types of student data include

- ***Personally Identifiable Information (PII)***: Information that is maintained in education records and includes direct identifiers, such as a student's name or identification number, and indirect identifiers, such as a student's date of birth or other information that can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information.
- ***Deidentified Data***: Data about individual students that has enough information removed that a student cannot be identified, such as data that has been subjected to statistical techniques to limit disclosure. Deidentified data may be published in reports about student achievement or shared with external researchers.
- ***Aggregate Data***: Data about groups of students, for example, data shared as part of a school's federal reporting requirements on topics such as attendance rates.
- ***Metadata***: Data that describes and gives information about other data, such as indicators on how much time a student spent on a test as opposed to their grade on the test.



TO LEARN MORE:

- Data Quality Campaign, What Is Student Data?

Why Use Student Data?

Student data may be collected for a number of purposes, including

- To improve a student's educational experience, including allowing educators to track student progress and plan appropriate interventions if or when needed;
- To protect a student's health and safety, including maintaining medical forms, allergy information, and emergency contact information;
- To fulfill a school's basic administrative functions, including collecting, maintaining, and reporting basic enrollment, attendance, and academic records for students; and
- To fulfill basic administrative functions of local, state, and federal governments, including tracking school and district performance, assessing how funding is used, and informing the public.

TO LEARN MORE:

- Data Quality Campaign, How Data Help Teachers

Who Uses Student Data?

Different types of education stakeholders collect and use student data to fulfill their roles and responsibilities:

- ***Students*** use their data to assess their current strengths and weaknesses, to set goals, and to track their progress, thereby taking ownership of their educational journey.
- ***Parents/Caretakers*** use student data to follow their children's learning, to partner with educators to provide support at school and at home, and to better advocate for their children.
- ***Teachers*** use student data to understand students' learning, to tailor lesson plans to individual students, and to assess student performance and outcomes.
- ***School and District Administrators*** use student data to understand the strengths and weaknesses of their education programs and curricula, to assess the resources they may need to drive improvements, and to report student performance and outcomes.
- ***State Departments of Education*** use student data to measure how schools and districts meet goals for students, to inform funding needs, and to report high-level data to the public and to federal offices.
- ***The US Department of Education*** uses aggregate student data to provide information to the public about performance and to measure how federal funds improve education.
- ***Education Technology Companies*** and other third-party service providers hired by schools and districts use student data to help schools and districts support students.
- ***Researchers*** use student data to study important educational research questions and to support data-informed decision-making.

TO LEARN MORE:

- Data Quality Campaign, Who Uses Student Data?

What Is Data Privacy?

Privacy is an amorphous concept, which people in different contexts define in various ways. One person may think of privacy as being alone in a private space, such as their bedroom. Another person may associate privacy with being free from surveillance, whether by their parents/caretakers, their schools, or the government. Some of the common conceptions of data privacy include

- Data privacy as a *fundamental right*. Individual privacy rights are recognized in the US Constitution, the UN Declaration of Human Rights, and in over 80 countries around the world. Privacy rights also provide the foundation for other important rights, including self-determination and free expression.
- Data privacy includes a person's *control* over how their personal information "flows" between them and any third parties (how it is used and shared).
- Data privacy is *subjective*, as each person has unique privacy preferences and expectations. What feels invasive or creepy to one person may be innovative or cool to another. Many factors influence these preferences and expectations, including a person's familiarity with the entity or person collecting their data, whether a person is from a marginalized community whose data has been used in inequitable ways, their cultural background, and their trust in data-holding organizations.
- Data privacy is *contextual*. Whether it is appropriate to use or share personal data in a particular manner depends on ever-evolving social and ethical norms and on legal frameworks. To ensure that people understand an education agency's or institution's community norms about data use, the agency or institution must communicate and engage directly with their community members.

Establishing and maintaining privacy, whether by being left alone or avoiding being watched, was relatively straightforward before the advent of digital technologies. Today, technologies such as smartphones, which people carry in their pockets, and the trackers that load invisibly online whenever people open a web page can make it feel like privacy no longer exists.

With the introduction of these technologies and their unprecedented ability to collect and use data, stakeholders have talked about the word "privacy" as a form of fairness and power. The more information that one person or organization has about another, the more that party may influence or exert power over the other. Data privacy protections help individuals and communities maintain their autonomy and freedom when their governments and other organizations use their information. For example, institutions, such as governments and companies, harvest and retain massive data sets on their citizens and users. This data is often collected from individuals without their knowledge or informed consent and can be used for purposes over which they have little to no control. In this context, data privacy helps to establish agreed-upon protections to affirm fairness, including the creation of transparent policies and practices that help correct power imbalances among the individual, the technology, and the institution.

TO LEARN MORE:

- Future of Privacy Forum, Nothing to Hide: Tools for Talking (and Listening) About Data Privacy for Integrated Data Systems

What Is Student Data Privacy?

Privacy, as a central component of fairness, often comes up in the educational context. **Student data privacy refers to the responsible, ethical, and equitable collection, use, sharing, and protection of student data**. Why is it so important to protect student data? Any type of data collection, use, or sharing entails potential short- and long-term risks. Those who have had a credit card compromised or personal information stolen are aware of the difficult ramifications of data collection and sharing gone awry. Just like toothpaste squeezed from a tube, once sensitive information is released, it is hard, if not impossible, to get it back where it belongs.

Because students—especially younger children—are not fully equipped to weigh the potential benefits and risks of data collection and use, they require special privacy protections. They are also at risk for more-acute harms, such as opportunity loss, that may not fully emerge until later in life. Data privacy protections can support students' success and give them agency over their information and education.

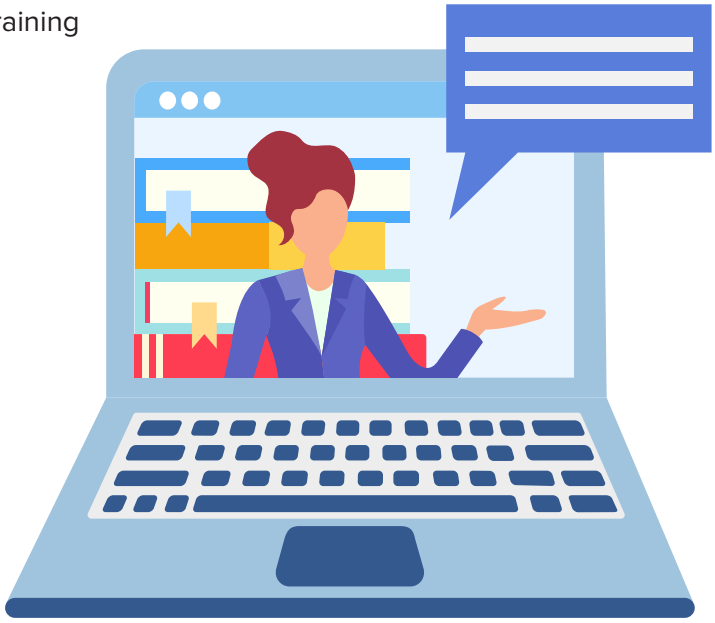
There are a few misconceptions about data privacy. First, seeking to protect data privacy does not mean preventing all others from learning information about an individual. On the contrary, data privacy is about creating conditions in which individuals will share their personal information because they trust that others will protect it. This is particularly important in the educational context, in which students rarely have a choice about whether to share their personal information with their education institution.

In addition, while data privacy and data security are closely related, a perfectly secure data system may still violate individual privacy if authorized users acting within an organization's or system's normal capabilities collect or use personal data in covert, unexpected, inappropriate, or inequitable ways.

Finally, student data privacy is not just another item to be checked off a list to ensure legal compliance, or a bureaucratic barrier to helping students excel in the classroom. Rather, data privacy is integral to data use that informs priorities and supports students in an ethical and equitable manner. School and district leaders should remember that, while student data can be immensely valuable to help improve teaching and learning, the misuse or unauthorized disclosure of student data can also put students and their families at risk.

TO LEARN MORE:

» Future of Privacy Forum, Student Privacy Training for Educators: Defining Privacy



What Are Student Data Privacy Risks and Harms?

When proper student data privacy protections are not in place, schools and districts face significant risks to their students, their schools, or districts. These risks fall into three main categories:

- ***Actual Harm:*** Students may suffer physical, emotional, or reputational harm due to unauthorized access to their personal information.
- ***Legal Consequences***: Schools and districts may face fines, lawsuits, or even imprisonment for their failure to comply with federal and state student privacy laws.
- ***Public Relations Disaster***: Even if schools and districts avoid data breaches and comply with legal requirements, the perception of unethical or irresponsible practices due to misinformation or lack of communication can result in a public relations disaster.

Actual harms to students can be further categorized into eight types:

- ***Commercialization***: Companies may access and use student data to target advertisements to students and build student profiles.
- ***Equity Concerns***: Students have varying access to devices or internet service, which has implications for the levels of safeguards in place and monitoring that occurs.
- ***Social Harm***: Revealing personal and sensitive student information can result in stigmatization and cyberbullying.
- ***Over-Surveillance***: Over-collection and monitoring of student data and online activity can have chilling effects, such as discouraging students' interest in learning or taking healthy risks.
- ***A Permanent Record***: This regards how long institutions retain records of events, specifically mistakes, potentially tethering students to their past in limiting or harmful ways.
- ***Loss of Opportunity***: Student data can be used to make decisions about students that can result in denials of opportunity.
- ***Age-Inappropriate Content***: Students may access inappropriate websites and online content.
- ***Safety***: Personal or otherwise sensitive information may be revealed that could endanger students' safety.

TO LEARN MORE:

- Future of Privacy Forum, Student Privacy Training for Educators: Why Protect Student Data
- Future of Privacy Forum, Student Privacy Training for Educators: Understanding and Reducing Risk
- Danielle Keats Citron and Daniel J. Solove, *Privacy Harms,* (February 9, 2021), GWU Legal Studies Research Paper No. 2021-11, GWU Law School Public Law Research Paper No. 2021-11, Accessed April 29, 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3782222.
- Enterprivacy Consulting Group, A Taxonomy of Privacy.

How Does Student Privacy Relate to Data Ethics and Data Equity?

From a data privacy perspective, responsible data use is more than compliance with laws and regulations and goes beyond basic assumptions of fairness. Student data privacy policies and practices must ensure ethical and equitable uses of data that minimize potential for harm and risk, especially to students from marginalized groups (e.g., students of color, students with disabilities, and students from lower socioeconomic backgrounds).

Data ethics and equity are related but different terms regarding how student data is used. Data ethics are the guiding principles for how stakeholders should govern, use, and protect data to minimize harm and risk. Examples of ethical data use include data governance policies and district practices that convey which data can be collected, how long data can be retained, who has access to data, and the purposes for which data is used. An ethical approach to data use includes policies that clearly distinguish appropriate and inappropriate data practices and communicate standards for data collection, use, protection, and sharing.

Data equity is dependent upon ethical policies and practices. What differentiates data equity from ethics is its focuses on using data to understand structural and systemic educational barriers to students' success and to take actions to improve those structures and systems. Equitable data practices include regular audits of data, data systems, and data practices to assess and remediate bias or discrimination (e.g., unequal surveillance and discipline of students of color or noncompliant ADA edtech use) and identifying and addressing achievement, resource, and opportunity gaps (e.g., unequal graduation rates, student access to technology, or teacher shortages). A data equity mindset includes students and their families in the responsible and ethical use of their data. In practice, this includes regular communication to understand students' needs and realities and regularly informing students of their rights related to data collection and use.

It is imperative to think beyond privacy and to incorporate appropriate and ethical data use. Some practices may not violate FERPA, but they may be unethical, inequitable, or inappropriate in some way, such as drawing inappropriate or unfounded conclusions, making inferences based on limited or biased data, using cognitive fallacies in reasoning, cherry picking results, using confirmation bias, and other poor practices. Minimizing harm, bias, and discrimination in systems and practices requires data use that is student-centered and grounded in privacy ethics and equity.

TO LEARN MORE:

- Urban Institute, Equitable Data Practice
- The Education Trust, Data Equity Walk Toolkit
- Ellen B. Mandinach and Edith S. Gummer, (Eds.), *The Ethical Use of Data in Education: Promoting Responsible Policies and Practices*, (2021), New York, NY: Teachers College Press.

What Are Key Federal Privacy Laws?

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 children's education records and restricts who can access and use student information. FERPA protects access to and sharing of a student's education record, which is all information directly related to a student's education. FERPA gives parents specific rights to their children's education records, and when a child turns 18, the rights belong directly to the student.

FERPA also permits schools to share information with a) another school system regarding a student's enrollment or transfer, b) specified officials for audit or evaluation purposes, c) appropriate parties in connection with a student's financial aid, d) organizations conducting certain studies for or on behalf of the school, e) accrediting organizations.

FERPA's "school official" exception allows schools to share information with parent volunteers, technology companies, and other vendors but only when these parties use the information for educational purposes directed by the school. 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 schools must give parents the opportunity to opt out.

TO LEARN MORE:

- US Department of Education, Student Privacy 101: FERPA
- ConnectSafely and Future of Privacy Forum, The Educator's Guide to Student Data Privacy
- US Department of Education, FERPA and Virtual Learning
- US Department of Education, Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices
- Future of Privacy Forum, Student Privacy Training for Educators: Adopting EdTech Privacy Vetting

PPRA. The ***Protection of Pupil Rights Amendment*** outlines process restrictions for when education institutions may ask students for information as part of federally funded surveys or evaluations. Specifically, PPRA requires parental notification and/or consent before minors can participate in school-administered surveys that reveal sensitive information. For example, schools may want to use surveys to better understand the social and emotional health of their students. They might also seek to understand students' needs and circumstances regarding issues such as internet and device access or food security. To administer such surveys, schools must be able to show parents the survey materials used, and parents must either opt in or opt out, depending on whether student participation is required and/or the survey addresses certain sensitive categories.

TO LEARN MORE:

- Future of Privacy Forum, FAQs: The Protection of Pupil Rights Amendment
- Future of Privacy Forum, Student Privacy Training for Educators: Student Surveys
- US Department of Education, Protection of Pupil Rights Amendment (PPRA) General Guidance

COPPA. The ***Children's Online Privacy Protection Act*** regulates information collected from 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 an educational context. This means a company can collect personal information from students only for a specified educational purpose and no other commercial purpose. Most schools have policies requiring school administrator approval before teachers can allow students to use certain apps and services. When companies collect information with the consent of a school official, the companies may keep the information only as long as necessary to achieve the educational purposes.

TO LEARN MORE:

- Common Sense Media, What Is COPPA?
- Federal Trade Commission, Complying with COPPA, Frequently Asked Questions
- Future of Privacy Forum, Student Privacy Training for Educators: Adopting EdTech Privacy Vetting

IDEA. The ***Individuals with Disabilities Education Act*** provides for a "free appropriate public education," including special education and services, for children with disabilities. To receive federal funding under IDEA, states must have systems in place to protect the confidentiality of personally identifiable information and must maintain parents' right to consent to the exchange of that information. IDEA also grants parents the right to examine records relating to their children's assessment, eligibility determination, and individualized education plan. In addition to granting parents access and deletion rights that are similar to those of FERPA, IDEA establishes a higher standard of confidentiality for the student records it covers, such as a student's individualized education plan.

TO LEARN MORE:

- US Department of Education, Individual with Disabilities Education Act

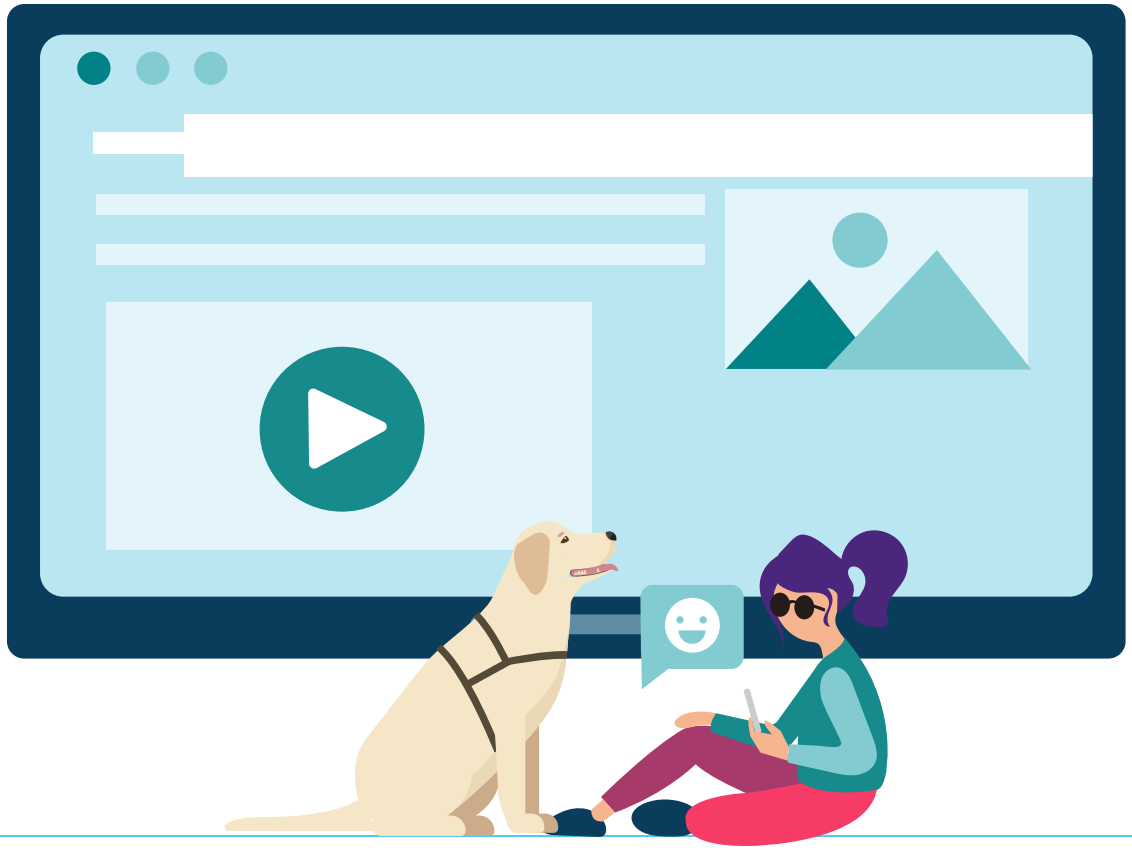
What Are Key District and School Policies?

Schools and districts have a number of policies that protect student data privacy. These policies include information that specifically apply to educators and should inform classroom practice and communication with students and families. The purpose of these policies is to support the school's legal and moral obligation to keep students' data safe. We have listed a number of policies below that your school or district may have. It is highly recommended to be familiar with these policies and consult as needed.

- Edtech Vetting and Adoption
- Posting Student Work
- District and Personal Social Media Use
- Directory Information
- Photos and Videos of Students
- Virtual Learning/Video Classrooms
- Protection of Pupil Rights Amendment (PPRA)
- Student and Parent Communication
- Data Destruction
- Parental Information Request
- Data Sharing with Community Organizations
- Data Breach
- Researcher Agreements

To learn the most important details about each of these policies and when to consult them, watch the following free video training:

- Future of Privacy Forum, Student Privacy Training for Educators: What Are Your School's Policies?



What Is a Culture of Privacy?

School and district leaders are key actors in protecting student data privacy, but they are not alone. Each group of education stakeholders has an important role to play to ensure responsible use and protection of student data. Schools and districts must work together with educators, parents/caretakers, and students to create a culture of privacy in which all parties understand the need to protect student data privacy and act accordingly. Building a culture of privacy requires understanding the legal landscape, a robust data governance program, streamlined vetting of edtech tools, trained educators and staff, and consistent communication.

- ***School and district leaders*** can establish robust student data privacy policies, procedures, and practices; properly train educators and staff handling student data; and facilitate meaningful two-way communications with parents/caretakers and students.
- ***Educators*** can build their professional capacity by learning about student data privacy; proactively share information with students and their families about the purpose and mechanisms of student data collection and use in the classroom; and take precautions to ensure that the tools they use adequately protect student data privacy.
- ***Parents/Caretakers*** can learn about laws that govern the collection and use of student data; understand parental rights related to those laws in order to act as partners in their children's educational journey and protect their children from potential data misuse or harm; advocate for robust student data privacy and data governance programs and training; and have conversations with their children about how to engage safely and responsibly online.
- ***Students*** can play an active role in protecting their data by developing skills to become good digital citizens, including managing their digital identities and reputations, engaging in positive, safe, legal, and ethical behavior online, and being aware of how their data is collected and used in the school environment.

TO LEARN MORE:

- Future of Privacy Forum, Student Privacy Training for Educators: Advocating for a Culture of Privacy
- Future of Privacy Forum, Student Privacy Communications Toolkit: For Schools & Districts

More Resources

- Privacy Technical Assistance Center (PTAC) is located within the US Department of Education's Student Privacy Policy Office (SPPO). In addition to providing resources regarding student privacy, legal compliance, and best practices, PTAC also operates a Student Privacy Help Desk, offering assistance on complex student privacy issues via phone or email.
- ConnectSafely and Future of Privacy Forum created The Educator's Guide to Student Data Privacy, which covers student data privacy topics such as how teachers can use technology in the classroom while protecting their students' privacy.
- Common Sense Media's Privacy Program evaluates the privacy policies of numerous learning tools, so that educators can make informed choices on the tools they use in the classroom. The Common Sense Privacy Program also provides training for educators on privacy and security.


FUTURE OF
PRIVACY
FORUM