Student Privacy Primer for School Leaders

JULY 2023

FUTURE OF PRIVACY FORUM

ABOUT THE FUTURE OF PRIVACY FORUM

The Future of Privacy Forum (FPF) is a nonprofit organization focused on how emerging technologies affect consumer privacy. FPF is based in Washington, DC, and includes an advisory board
comprised of leading figures from industry, academia, law, and advocacy groups.

FPF's Youth & Education Privacy program works to protect child and student privacy while allowing for data and technology use that can help young people learn, grow, develop, and succeed. FPF works with stakeholders from practitioners to policymakers, providing technical assistance, resources, trend analysis, and training.
FPF's Youth and Education Privacy team runs Student Privacy Compass, the one-stop-shop resource site on all things related to student privacy.

AUTHORS

Ellen B. Mandinach, PhD
Senior Research Scientist
WestEd

Jim Siegl
Senior Technologist,
Youth & Education Privacy
Future of Privacy Forum

Jo Beth Jimmerson, Ph.D.
Professor, Educational Leadership & Higher Education
Texas Christian University

David Sallay
Director,
Youth & Education Privacy
Future of Privacy Forum

ACKNOWLEDGEMENTS

FPF thanks the following individuals for contributing their time, insight, and work in providing feedback on the information in these resources:

Jamie Gorosh
Senior Counsel,
Youth & Education Privacy
Future of Privacy Forum

Laura Amortegui
Program Manager,
Youth & Education Privacy
Future of Privacy Forum

Bailey Sanchez
Senior Counsel,
Youth & Education Privacy
Future of Privacy Forum

TABLE OF CONTENTS

Introduction

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.

Overview of Data Privacy

Why is Data Privacy Important?

Educators use a plethora of data in their everyday practice. Using a range of data helps inform decision-making and ensure that the decisions are based on evidence. Data come in many forms and have different meanings to different educators. Data may be used for accountability and compliance purposes, or they may be used for continuous improvement. (In fact, due to the historical and tight coupling of data use with accountability system data, some educators might not even realize how much data they generate and can use to inform practice.)

Data may be longitudinal or snapshot, capturing aspects of development over time or systemic health, or data may be part of the moment-to-moment moves teachers and principals make day in and day out as they work with students and with each other. Data may be summative or formative. They may be quantitative or qualitative. Data may inform across levels of the education system, from the classroom to the school to the district to the state and the federal level. The same data may have different purposes based on if you are a classroom teacher, a building administrator, or a district leader. Data are complex.

Despite the complexity, two grounding principles apply regardless of the data. First, data range far beyond quantitative test scores that provide student performance indicators. Data also include socio-emotional, affective, behavioral, medical, attitudinal, transportation, socio-economic status, and much more. Second, data must be used ethically and in line with policy/legal requirements and an acknowledgment of the importance of protecting student data privacy.

Understanding & Protecting Student Data Privacy: The School Leader's Role

Educators at all levels–from the classroom to campus leaders to district leaders, must know how to use data effectively and responsibly. Leaders are responsible for building the capacity to use data ethically and well among those under their supervision. This means that leaders must be data literate (Mandinach & Gummer, 2016) and must understand concepts such as data privacy and data ethics in addition to understanding and enacting grounding concepts of school leadership. The objective of this document and the accompanying scenarios is to help educators gain insights into and knowledge of data privacy and data ethics and to help leaders grow their own capacity for navigating ethical and legal approaches to leading data use in their respective contexts.

The Family Educational Rights and Privacy Act (FERPA) is the educator's north star for the protection of student data privacy. At the same time, it is not the only legislation that governs how data may be collected, stored, used, and shared: other regulations may also apply, depending on context. It is incumbent upon educators, especially school and district leaders, to understand FERPA (and other laws, such as COPPA and PPRA, which apply to particular situations in schools). Educational leaders need to understand pertinent laws and how they apply to educational practice in their venues; if nothing else, they need to have enough familiarity with data privacy laws and concepts to understand when the waters are getting deep enough and the issues complex enough, that they need to engage with other personnel, like IT professionals and district legal counsel.

In addition to formal regulations that impact responsible data use, data use has an ethical component. It is important to use data effectively, but data must also be used appropriately, taking into consideration many aspects of ethics (Mandinach & Gummer, 2021). A major component of ethics is equity. Some approaches to data use have been shown to marginalize some of the most vulnerable groups of students

(Datnow, 2017; Datnow & Park, 2018). This is most common when data are used strictly for accountability system purposes, which can invite attempts to "game the system" (see Booher-Jennings, 2005; Daly, 2009; and Marsh et al., 2016 for some examples). Research has long underscored the role of the school and district leaders in modeling and setting the tone for data use (e.g., Anderson et al., 2010; Datnow et al., 2017; Jimerson et al., 2021; Marsh et al., 2016; Schildkamp, 2019). As the school leader says and does, so often does that become the norm for data use at the campus level or throughout a district. This is why leaders must have a firm understanding of data privacy and ethics issues and why it is critical for leaders to live out these principles in their day-to-day practice.

Therefore, educators need to understand the ramifications of data use that can lead to equity issues in terms of systematic barriers that impede student success. Proper processes, policies, and protections must be in place to ensure effective and responsible data use. Without such protections, there is potential for harmful consequences and harm.

For the purposes of this primer, we differentiate between two kinds of data: student data and administrative function data. As an administrator or individual who helps prepare educational leadership candidates, student data are perhaps the most commonly used and referenced data in a school or district. As you will see, many regulations pertain to such data. These data are not only used to inform instructional practices but also serve to inform administrative decisions. That said, there also are data primarily used for administrative purposes. Administrators must understand the proper and ethical use of both forms of data. We address both forms of data, providing examples and guidance for use.

Student Data

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 requested or required when registering a student for school;
- Grades, test scores, attendance, discipline and health records, and college and career goals that are tracked to help schools follow the progression of a student throughout their educational career;
- Recorded observational data about a student's behavior, motivation, or interests generated by educators throughout the school day;
- Student performance, time-on-task, and outcomes generated through homework, learning applications, and standardized tests; and
- Data that helps schools understand and assess the needs of students 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

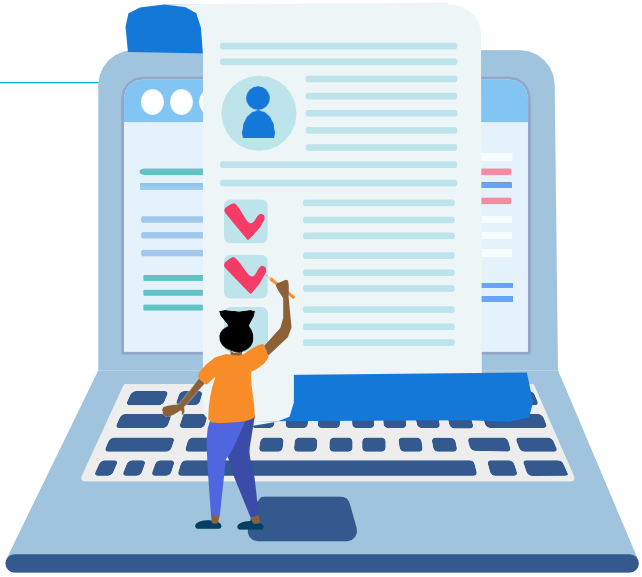
- ***Personally Identifiable Information (PII)***: Information that is maintained in education records and includes direct identifiers, such as a student's name or identification number, and indirect identifiers, such as a student's date of birth or other information

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 are improving education.
- Education Technology Companies and other third-party service providers hired by the school or district 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?

Administrative Data

What are Administrative Data?

Beyond data to inform instruction and student data, schools and districts collect and use many data sources that inform administrative functions. Administrators use such data to make decisions about the functions of a school and district. Examples of such data include decisions that pertain to:

- Curricula, to examine the efficacy of particular curricula and make decisions about the adoption of new texts, curricula, and materials;
- Employment, hiring, and the evaluations, to determine merit pay, promotions, tenure, job openings, and need for staffing decisions;
- Transportation, to examine the efficiency of bus routes to minimize costs of bussing; and
- Food Services, to determine expenditures for meals, free and reduced meals, and staffing.

Why Use Administrative Data?

Administrative decisions often require student-level performance data, PII, or other student data forms. But administrative data reach beyond student data to inform the decisions and functions noted above. School and district leaders must make decisions about personnel and staffing, resource allocation, and general educational functioning such as the provision of medical, transportation, food, security, and other services. Such decisions require a broad scope of data that informs decisions that maintain the district's effective and efficient functioning.

Who Uses Administrative Data?

School and district leaders, depending on their roles, need access to and use diverse sources of data to inform their own practice to address various types of decision-making.

- ***School Leaders*** use many forms of data to examine the functioning of their building, including hiring practices, curricula, program efficacy, student performance, trends in attendance, and more. Some decisions focus on continuous improvement while others focus more on accountability and compliance metrics.
- ***Curriculum Coordinators and Coaches*** use data to determine the efficacy of existing curricula or make decisions about adopting new materials. They may use student data to make these decisions. The data can be at the aggregate level or also to make decisions at the individual student level.
- ***Other Building Staff*** use various forms of data to inform their decision-making. For example, food service staff need access to Free or Reduced Priced Lunch status to

determine the provision of meals to low-income students.

- ***Guidance Counselors*** use student-level data to counsel individual students and various administrative data to inform more aggregate-level analyses. These might include counseling about applications for higher education or program trends.
- ***Central Office Staff***, depending on role and function, use diverse data sources to make administrative decisions. Such decisions might include the transportation director analyzing bus routes to determine efficiency, the food services director determining how many students qualify for free or reduced meals, and the security department analyzing trends in disciplinary infractions.
- ***Superintendents*** use diverse data sources to examine the effective and efficient functioning of their district, both for continuous improvement and to meet compliance and accountability metrics.

What is Data Privacy?

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

- Data privacy as a *fundamental right*. Individual privacy rights are recognized in the U.S. 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 everyone 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 historically 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 educational agency or institution's community's norms about data use, it is essential for that agency or institution to communicate and engage directly with community members.

Despite the varied conceptions, establishing and maintaining privacy, whether by being left alone or avoiding being watched, was relatively straightforward before the advent of digital technologies. Today, technologies, like smartphones that people carry in their pockets and the trackers that load invisibly online whenever people open a webpage, 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 has been used as proxy for talking about fairness and power. The more information 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. These data are 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 instance, privacy is not only a definition. Still, it plays a role in establishing agreed-upon protections to affirm fairness, including creating transparent policies and practices that help correct power imbalances between the individual, the technology, and the institution. 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

Why Student Data Privacy Matters

Privacy, as a central fairness component, often comes up in the educational context. ***Student data privacy refers to the ethical and equitable collection, use, sharing, and protection of student data.*** Why is it so important to protect student data? Data collection, use, or sharing entails potential short- and long-term risks. Those who have had a credit card compromised or personal information stolen know the difficult ramifications of data collection and sharing gone awry. Like toothpaste in 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 be fully realized or discovered until later in life. Data Privacy protections can support student success and give them agency over their own information and education.

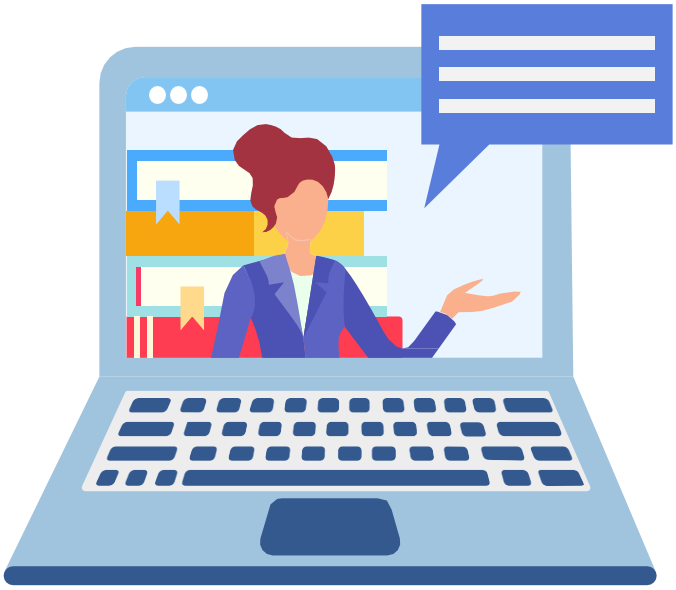
There are a few misconceptions about data privacy. First, seeking to protect data privacy does not mean preventing all others from learning information about an individual. On the contrary, data privacy is about creating conditions where individuals share their personal information because they trust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

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

Finally, it is important to remember that privacy is not just another item to be checked off a list to ensure legal compliance to be legally compliant, or a bureaucratic barrier to helping students excel in the classroom. Rather, data privacy is integral to effectively using data to inform priorities and support students ethically and equitably. 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 Privacy Risks and Harms?

When proper student data privacy protections are not in place, schools and districts face significant risks to their students or their school or district that can be categorized into three main buckets.

- ***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 failing 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 a lack of communication alone can result in a public relations disaster.

Actual harms experienced by students can be further categorized into these eight potential harms:

- **Commercialization:** Companies may access and use student data to target student advertisements and build student profiles.
- **Equity Concerns:** Students have varying access to devices or internet service, which has implications for 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 on students.
- **A Permanent Record:** This regards how long records of events, specifically mistakes, are retained.
- **Loss of Opportunity:** Student data can be used to make decisions about students and, specifically, 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,
- Enterprivacy Consulting Group, A Taxonomy of Privacy.

How Does Student Privacy Relate to Data Ethics?

Data ethics is an overarching concept of which data privacy is a component. Data ethics pertains to the appropriate and responsible use of data, not just the protection of the privacy and confidentiality of data. Data ethics are about using the "right" data with the "right" analytics to draw appropriate inferences and make the "right" decisions. From a privacy perspective, responsible data use is more than compliance with the 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 the potential for harm or risk, especially to students from marginalized groups (e.g., students of color, students with disabilities, or students from lower socio-economic backgrounds).

Data ethics and equity are related, but different terms reference how student data is used. Data ethics are the guiding principles for how data should be governed, used, and protected to minimize harm and risk. Examples of ethical data use include data governance policies and practices by school districts that convey what 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 delineate appropriate versus 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 focus on using data to understand structural and systemic educational barriers to student success and to take actions to mitigate bias and 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 non-compliant ADA edtech use) and identifying and addressing achievement, resource, and opportunity gaps (e.g., unequal graduation rates, student access to technology, or school district teacher shortages). A data equity mindset includes the student (and their family) 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 to appropriate and ethical data use. Situations 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 any number of other poor practices. Minimizing harm, bias, and discrimination in systems and in practices requires data use that is student-centered and grounded in privacy ethics and equity. It also requires assuming an asset model and a whole-child perspective.

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.
- Ellen B. Mandinach and Edith S. Gummer (in preparation). Shining light on ethical uses of data in education: Emerging importance: Educational Researcher.

How Does Student Privacy Relate to Data Ethics and 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, and 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

Ten Steps to Privacy: Disclosing Records Under FERPA

In general, the Family Educational Rights and Privacy Act (FERPA) requires schools to obtain written parental consent before disclosing information derived from student education records. Several exceptions to this rule allow schools to share information without prior consent. Each exception specifies rules or conditions that must be met before the disclosure. Schools will use some exceptions frequently, possibly daily (school official exception), whereas others will be used infrequently (accreditation exception). For a summary of following the most common FERPA exceptions, refer to this cheat sheet from the Privacy Technical Assistance Center (PTAC). For a complete list of exceptions, see 20 USC §1232g(b)(1)(A) through (L) with detailed explanations on how to follow the exceptions in 34 CFR Subpart D.

Schools are not required ever to use the exceptions and could get written consent in every case. In practice, however, schools should follow an exception when they can. For example, say the school is sharing information with a learning management system (LMS) to provide content to students. If a parent does not provide consent, it effectively bars the student from accessing the content (creating an unnecessary inequity). As a good rule of thumb, ask yourself if the average parent in your community would find the disclosure surprising or unexpected. In the case of an LMS, probably not (most parents expect schools to use technology to provide content to students). When the average parent would find the disclosure to be unexpected or surprising, that is a better fit for requiring consent before the disclosure. In these cases, open conversations about data usage with parent stakeholders and other members of the school community is the best way to decide how to proceed.

To quickly learn lessons from others and best practices, we have reviewed FERPA itself, complaint letters to the US Department of Education (which were released as part of a Freedom of Information Act request from the Electronic Privacy Information Center), Dear Colleague letters from the US Department of Education, and privacy frameworks such as NIST Appendix J and the Generally Accepted Privacy Principles (GAPP). We have condensed all this information into the following ten steps, which you can begin to follow to help ensure your compliance with FERPA.

1. Make your consent forms clear. When collecting consent from parents, the school must

- specify the records to be disclosed,
- explain the purpose of the disclosure, and
- identify to whom the disclosure will be made to.

For the consent to be valid, it must be signed by the parent or eligible student and dated. There is no requirement for checkboxes or anything similar. In fact, if the choice is a simple yes/no, checkboxes can add a potential layer of confusion. For example, some consent forms might end with this:

- **Yes,** I consent to have my student's data disclosed
- **No,** I do not consent to have my student's data disclosed

Imagine viewing this from the parent's perspective. Is this an opt-in or an opt-out? If the parent doesn't return the form, is their consent implied (or is their lack of consent implied)? What if they return the form signed and dated, but didn't check any of the boxes? How will the school interpret it? In these cases, the checkboxes don't add as much clarity as simply stating something like this: "by signing and dating this document, I affirm my consent to having my student's data disclosed."

Electronic consent is also valid, provided that you have authenticated the parent's identity (see also NIST, Appendix J, IP-1, and the Generally Accepted Privacy Principles 3.0 for more on consent).

2. Know which information is not protected from disclosure under FERPA. FERPA protects education records, which are records that directly relate to a student and that are maintained by the school or the school's agent. It does not protect all information an educator might know about a student. For example,

observations about a student generally are not covered since they are not maintained by the school on a record. Information that is known about a student, in general, would also not be covered. Furthermore, K–12 schools should know about the following records, which are also excluded from prohibitions on disclosure:

- Law enforcement records, or records created and maintained by the school's designated law enforcement unit for a law enforcement purpose
- Student employee records (unless the student's employment is a direct result of their being a student)
- Alumni records, that is, records created about a student who no longer attends the school and that do not directly relate to their attendance as a student
- Grades on peer-graded assignments before they are entered in the grade book

As a rule of thumb, before disclosing information, ask yourself which record it is being disclosed from. If you cannot name a record maintained by the school (e.g., because it is an observation or maintained by someone else) or it is one of the items listed above, then it is not protected and can be disclosed without consent or an exception.

3. Provide parents and eligible students with notice (and actually follow your policies). FERPA requires that schools include information about disclosure policies in their annual FERPA notice. Minimally, this should include an explanation of how the school determines who is a school official with legitimate educational interest and notice that the school will disclose records in cases of student transfer. It may also explain all of the exceptions under FERPA or more detailed local policies. The key is to make sure that you follow whatever it is you tell eligible students and parents. For example, in one case, a university shared student information with a professor emeritus, and the US Department of Education believed a professor emeritus could be designated as a school official; however, the university had not explicitly done so in their notice. As a result, the university said they would amend their notice to reflect their practice more accurately.

4. Go out of your way to explain the school official exception. Parental complaints are the primary enforcement trigger under FERPA; therefore, the more likely a parent is to notice a potential FERPA violation, the more likely they are to file a complaint. When incidents occur—like a dispute with a teacher (say the student is accused of cheating), bullying, or a fight on campus—parents will suddenly take a great interest in your record practices. Which record practice is a parent most likely to notice? Chances are, the ones that are visible and that involve having direct interactions with the school, which is why having a clear policy on how you define who is a school official with a legitimate educational interest is so important. Many FERPA complaints relate to the complainant feeling that an individual that received records was out of scope and did not in fact have a legitimate educational interest in the record. In one case, a student felt coerced to have another teacher in the room to function as a witness when discussing a grade appeal. In a similar case, the school had their lawyer and several other individuals the parent did not know sit in during an IEP meeting, despite the parent's protests.

Officially, FERPA only requires that eligible students and parents receive a notice annually that explains their rights under the law and how the school will determine who is a school official with legitimate educational interest. In practice, this will look like a list of positions or groups that could be school officials (see the US Department of Education's model annual notice as an example). In the examples above where the eligible student or parent felt coerced to discuss information with an individual they did not know, this could have been an opportunity for the school to remind the parent of their data policies and right under FERPA. For example, they could have shown the parent that their lawyer was designated as a school official and explained their legitimate educational interest in being in attendance in the meeting. Such proactive attempts to explain data policies can help alleviate confusion and prevent a parent from filing a complaint with the US Department of Education.

5. Know what can be shared with other students. Schools sometimes want to claim that if student information is shared in the classroom or elsewhere on campus, then it isn't really a disclosure; however,

there is no exception to FERPA's consent rule that allows this. It is the school's obligation under FERPA to ensure that information that is derived from education records is not disclosed, even to other students. There are multiple cases of FERPA complaints where disclosures were inappropriately made to other students. Some noteworthy examples are as follows:

- the student alleged that private, graded material had been improperly disclosed for the sole purpose of being ridiculed and mocked before classmates.
- a school counselor shared confidential medical information about a student to the student's friends so as to coerce them not to play with him anymore.
- the school principal revealed to the entire student body during an assembly that a student had a form of autism that made him aggressive, and if they saw him hurting himself or others, they should report it.
- the school took high school students on a field trip to a local university, where they had the students self-sort based on if they had passed the state summative assessment. They were then taken on very different field trips.

Other examples involve data walls, where student information is tracked on a display or wall in the room. Depending on if the information appearing on the data wall is derived from information in a student's education record, it could be a violation of FERPA. So having students publicly track the number of books they have read is generally permitted, whereas having students publicly track their scores from the teacher's grade book on their literacy assessment would not (unless parental consent was obtained).

6. Assign responsibilities and train accordingly. Though FERPA provides several exceptions to the consent rule, not everyone at the school should be authorized to use every exception (e.g., it is highly unlikely that the school bus driver will be making disclosures using the financial aid exception). Designate who at the school is authorized to make specific disclosures. You can do this by making a list of the different types of school officials on one side and a list of FERPA exceptions on the other. An example might look like this:

Employee	School Official	Directory Information	Studies	Audit/ Evaluation	Health/ Safety	Law Enforcement
Teacher	with other staff	X				
Admin or their delegate	X Approve 3rd parties as school officials	X	X	X	X	X
Front Desk	with other staff	X			X	

After determining who may share under which circumstances, ensure that those educators are trained not just on how to properly follow the exception but also on whom to escalate issues to that they are not authorized to resolve. In the above example, teachers have been authorized to share with other teachers using the school official exception, but not websites, so they would need to be trained on whom to contact and the approval process for cases when they find a website they want to use (see also NIST, Appendix J, AR-5 for more on training).

7. Track disclosures and requests for disclosures. In 34 CFR § 99.32, FERPA requires that schools keep a record of all disclosures and requests for disclosures of student records, including the recipient's name and the legitimate purpose they have in the information. There are a few exceptions to this rule:

- when disclosing using the school official exception

- when written consent was obtained from the parent or eligible student
- when using the directory information exception
- when disclosing to comply with a judicial order or lawfully issued a subpoena that explicitly indicates that the contents of the subpoena are not to be disclosed

Eligible students and parents have the right to inspect this record, meaning if they ask to see whom the school is disclosing their records to, the school must comply (see also NIST, Appendix J, AR-8).

8. Know your state laws too. A few exceptions within FERPA depend on state laws. For example, the Juvenile Justice Services exception can only be used in accordance with requirements set out in state law (so if your state does not have a law that allows it, you may not use this exception). You should also know your state's requirements under the Child Abuse Prevention and Treatment Act (CAPTA) as these will generally supersede any requirements under FERPA. Furthermore, from 2013 to 2019, 41 states have passed 126 laws that affect student privacy, in many cases adding additional requirements before data can be shared, particularly with educational websites.

At the same time, just because a state law authorizes data sharing doesn't mean it supersedes FERPA. There is no "other state agency" exception that would allow a school, district, or state educational agency to disclose records just because a state law allows it. Rather, the school will need to look at the existing exceptions and determine which one is the best fit (depending on the circumstances, school official or audit/evaluation may apply). The US Department of Education has this guidance document on using FERPA to share with other state agencies as part of an integrated data system. Even if this isn't your specific use case, the same interpretation of FERPA may apply.

9. Disclose the least amount of data possible. Prior to sharing student data, you should determine the minimum amount of data that are relevant and necessary to accomplish the goal of the disclosure. For example, say you are sharing information with an educational website. Just because the website asks for information doesn't mean you have to give it. If the field is marked as optional or if the educational purpose is not clear (e.g., if a calculator website wants to know the student's gender), then there is no reason to share. Very often, websites will ask for a student's name simply to provide more personalization. If you determine that you do not need to disclose any direct identifiers, you could also follow a process called tokenization, which could be as simple as assigning a generic identifier to each student (e.g., student01, student02, etc.) that could not be traced back to the original student.

When de-identifying student-level data to release publicly, remember that the standard is if a reasonable person in the school community, who does not have personal knowledge of the circumstances, could re-identify that student with reasonable certainty. This means that in many smaller communities (such as charter schools or rural school districts), sharing small data sets or even aggregating data may be insufficient to protect student privacy. The US Department of Education's Response to Louisiana on Enrollment Data and Disclosure Avoidance provides additional information on best practices for avoiding re-identification when disclosing aggregated data.

10. Think about assurances. Several FERPA exceptions require a written agreement between the school and the data recipient. For example, the audit/evaluation and studies exceptions require that the written agreement discuss the purpose and scope of the disclosure and provisions for destroying the data after that purpose is completed. The school official exception includes a requirement that the school maintain direct control over the data with respect to its use and maintenance. Since there are many different types of school officials, this direct control will look different for different parties. Volunteers, for example, may be asked to sign a nondisclosure agreement (NDA). Educational websites and apps generally have terms of service and privacy policies. Ideally, these would be reviewed prior to usage, but realistically reviewing everything used by the school would be prohibitively time-consuming. Because of this, several schools and states around the country have opted to create a standard data privacy agreement (DPA), which is distributed via a group like the Student Data Privacy Consortium (SDPC).

For riskier partnerships (such as ones where the contract is more costly or the recipient receives large amounts of sensitive data), the school may want to include language related to auditing and monitoring in

these agreements. Generally Accepted Privacy Principle 7.2.2 discusses how this does not need to be an invasive on-site audit in every case. Rather, it could also be something more practical and scalable, like providing the school with a brief annual self-assessment of their privacy and security measures, completing a questionnaire to provide more detail, or supplying the school with a Services and Organization Controls (SOC) 2 report or evidence that they have received a security certification, such as ISO 27001.

Disclosures under FERPA may seem intimidating since there are several requirements and exceptions to the rules. These rules are ultimately in place to achieve a balance between parent and student rights regarding data and the school's need to function and provide services. By following the ten steps listed here, your confidence in your ability to comply with the law will increase, and your school will be able to ensure better that data can be used to improve educational outcomes and students' lives while concomitantly respecting their privacy.

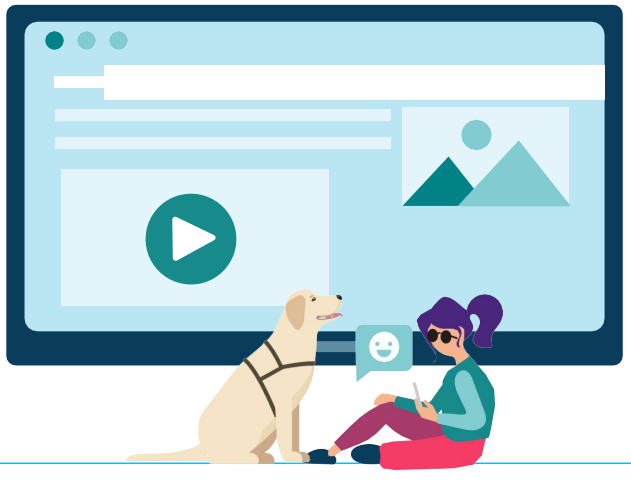
What Are Key District and School Policies?

Schools and districts have several policies that protect student data privacy. These policies include information that specifically applies 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 several 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 Data Governance?

Student privacy is best protected by schools and districts with a data governance plan. Data governance refers to the policies, practices, and procedures allowing organizations to effectively manage their data. Considering the amount and sensitivity of the personal information collected, used, and maintained by schools and districts, establishing a robust data governance program is critical to protect student privacy and to ensuring all stakeholders are engaged and invested in creating a culture of privacy.

Without a clearly articulated and well-executed data governance program, school and district leaders may face suspicion and opposition to student data use for legitimate educational purposes. Prioritizing data governance can dispel some suspicion by signaling a commitment to protecting student privacy. Moreover, by addressing data governance concerns proactively, schools and districts can improve their efforts to help students succeed through the responsible use of student data.

This section identifies some key elements of a data governance program and important student privacy policies and procedures for schools and districts.

Essential characteristics of an effective data governance program include:

- Creating privacy policies that protect and secure student data; clearly delineate legitimate users of student data and appropriate mechanisms for sharing data; and ensure ethical and equitable use of data, technologies, and privacy protections;
- Helping ensure that education stakeholders – including administrators, educators, parents, and students – understand what data is collected, for what purpose, and how it will be protected;
- Ensuring that data collection processes follow all federal, state, and local laws and regulations;
- Properly training and clarifying roles and responsibilities of those handling student data; and
- Providing accountability and transparency through clear documentation of roles, policies, and procedures and continuous engagement with education stakeholders.

If your school or district does not yet have a data governance program in place, the Forum Guide to Data Governance from National Center for Education Statistics (NCES) provides a comprehensive review of important elements to include in an effective data governance program that addresses both ethical and equitable student privacy and security requirements and the need for student data accessibility and sharing.

Some necessary student privacy policies and procedures include:

- Providing parents with an Annual Notice of Rights required under the Family Educational Rights and Privacy Act (FERPA) that includes notification of and procedures to exercise the right to inspect, review, and amend their student's education records;
- Creating procedures for compliance with the Protection of Pupil Rights Amendment (PPRA), including reviewing student surveys, providing notice to parents, and obtaining consent when necessary;
- Establishing policies and procedures for the approval of edtech tools that collect, store, and use student data;

- Requiring periodic privacy and security training for educators and staff with access to education records; and
- Adopting a security incident response plan that includes procedures for identifying, containing, mitigating, reporting, and communicating security incidents.

The Consortium for School Networking's (CoSN) Trusted Learning From the Ground Up: Fundamental Data Governance Policies and Procedures is also a valuable resource for schools and districts beginning to establish their data governance programs. The resource includes a checklist for inventorying existing data protection policies and procedures, presenting an opportunity to identify gaps that may inadvertently placing student privacy at risk. CoSN's Trusted Learning Environment (TLE) seal is also an option for districts seeking peer feedback on their data governance policies and practices.

Data governance programs can help build trust by establishing and articulating student privacy policies and practices and holding schools and districts accountable. However, data privacy policies are often complex and difficult for the layperson to understand. With that in mind, schools and districts should not only write policies in plain language but also clearly communicate the values that guide their decision-making. Educators, parents, and students need clear and easy-to-understand messages from schools and districts that convey a commitment to acting in accordance with ethical and equitable student privacy principles and that outline the school's or district's roles and responsibilities in adhering to and upholding them.

To aid in creating an understandable and useful data governance program, schools and districts should encourage educators, parents, and students to participate in the process by inviting them to sit in committee meetings, assist in drafting principles and policies, and report back how data governance is used in practice. Considering the organizational and educational contexts and engaging stakeholders will encourage greater participation in and adherence to privacy principles and policies. Further, it sets a baseline for establishing shared values and building a meaningful culture of privacy.

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 sharing information with students and their families about the purpose and mechanisms of student data collection and use in the classroom, and taking 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

Additional 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.