

Student Privacy Communications Toolkit

FOR SCHOOLS & DISTRICTS



JANUARY 2021



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

Jasmine Park
Policy Fellow, Youth & Education Privacy
Future of Privacy Forum

Amelia Vance
Director of Youth & Education Privacy
Future of Privacy Forum

Carrie Klein
Senior Fellow, Youth & Education Privacy
Future of Privacy Forum

Anisha Reddy
Policy Counsel, Youth & Education Privacy
Future of Privacy Forum

Juliana Cotto
Policy Fellow, Youth & Education Privacy
Future of Privacy Forum

Alexandra Sollberger
Principal & Director of Public Relations
Stones River Group

Ann Waller Curtis
Associate
Stones River Group

Jennifer Triplett
Associate
Stones River Group

ACKNOWLEDGEMENTS

FPF thanks the following individuals and their respective organizations for contributing their time, insight, and work in providing feedback on the information in this toolkit:

Fagen Friedman & Fulfrost, LLP

Andrea Tejedor
Assistant Superintendent for Curriculum,
Instruction & Technology
*Highland Falls-Fort Montgomery
Central School District*

Jim Siegl
Technology Architect
Fairfax County Public Schools

Data Quality Campaign

Julie Tonsing-Meyer
Associate Professor of Education
McKendree University

Sharon Thomas
Associate General Counsel I
Los Angeles Unified School District

Susan Bearden
Chief Innovation Officer
Consortium for School Networking (CoSN)

Illustrations courtesy Shutterstock/VectorMine

About the Future of Privacy Forum	2
Acknowledgments	2
Introduction	4
Student Privacy Primer	5
What is Student Data?	5
Why Use Student Data?	7
Who Uses Student Data?	7
What is Student Privacy?	7
What is Data Governance?	9
What is a Culture of Privacy?	10
Developing a Communications Strategy	12
Setting Goals	12
Creating a Communications Roadmap	13
Communications Best Practices	13
Use Clear Language	14
Consider Your Audience	15
Communicate to Establish Trust	15
Prioritize Equity and Engage Inclusively	15
Creating a Student Privacy Website	16
Talking to Parents	17
Elevator Speech for Talking with Parents	17
Talking Points to Use with Parents	18
Parental Rights	19
Back-to-School Letter	19
Educational Technology Consent Form	20
Online Learning: Monitoring Attendance and Student Engagement	21
Sample Parental Notice	21
Online Learning: Behavioral, Social, and Emotional Learning Surveys	21
Consent Form	22
Parents as Partners in Protecting Student Privacy	23
Sample Parent Letter	23
Sample Text Messages to Parents	23
Talking to Educators	24
Elevator Speech for Talking with Educators	24
Talking Points to Use with Educators	25
Evaluating Edtech Tools	25
Evaluating EdTech Tools for Privacy Checklist	26
Email Template to Educators	27
Practice Privacy When Using Edtech with Students	28
Recording Video Classes	28
Talking to Students	29
Elevator Speech for Talking to Students	30
Guiding Questions for Use with Students	30
Responsible Use of Technology Policy	31
Sample Responsible Use of Technology Policy	31
Online Learning: Monitoring Attendance and Student Engagement	32
Sample Student Notice	32
Conclusion	33
Additional Resources	33
Student Privacy	33
Data Governance	33
Model Communications Tools	33
Endnotes	34
References	37

Across the country, our K-12 education system is increasingly reliant upon data, technology, and online tools to identify opportunities to better support students, to develop policies and strategies to improve teaching and learning, and to inform the equitable allocation of education resources. The COVID-19 pandemic and subsequent school closures have expedited and expanded the use of educational technology tools to continue learning remotely. Switching from an in-person school environment to “classrooms in the cloud” heightens the pressure on schools and districts to protect student privacy, as more student data is collected, used, and potentially exposed. In addition to ensuring strong student privacy, safety, and security policies and practices are in place, this shift requires effective communication with stakeholders about student data collection and use.

School and district leaders must actively listen to and address educator, parent¹, and student concerns by creating spaces designed to inform, educate, and address student privacy questions. Alongside a robust student privacy program, schools and districts should develop a clear and comprehensive communications strategy to share information on student data collection and use and student privacy policies. They must also be particularly attuned to the challenges families with limited access to internet or technology, those students and families using assistive technologies for communications, and non-native English speakers face when accessing these communications.

Proactively communicating and engaging with educators, parents, and students creates opportunities to build trust and partnerships that can cultivate a culture of privacy protection. These

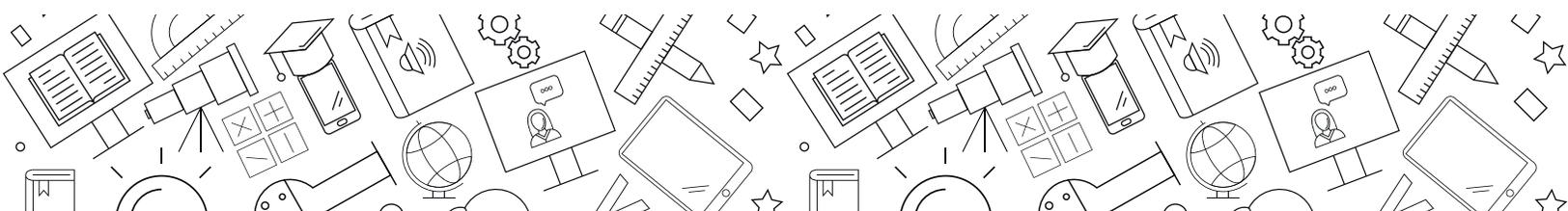
efforts also work to reduce privacy risks and to instill an appreciation for the value of student data to support student success. The Future of Privacy Forum (FPF) has developed this *Student Privacy Communications Toolkit: For Schools and Districts* to help school and district leaders have productive conversations with educators, parents, and students about ethical and equitable student privacy policies in their efforts to build trust and develop a culture of privacy.

While some schools and districts have well-established student privacy programs and policies with dedicated staff and resources, others are just beginning their student privacy journeys. Recognizing that there is no one-size-fits-all approach, this toolkit is intended to be adapted based on the needs or circumstances of an individual school or district. Each section will provide an overview of student privacy issues, examples of adaptable communication tools, and references to other resources to learn more about student privacy and data governance.

We hope you will use this toolkit to better understand the value of student data, inform privacy practices in an educational setting, raise awareness of the risks and challenges that come with increased data collection, take steps to help safeguard student information, and create a culture of privacy in your schools and districts.

We encourage you to visit www.StudentPrivacyCompass.org for additional updates, resources, analyses, and professional development materials. You can also follow us on Twitter (@SPPrivacyCompass) for real-time updates on our work. Reach out to us with suggestions for other resources that might be useful or any questions at: <https://studentprivacycompass.org/contact-us/>.

¹ In this toolkit, the term “parents” is inclusive of parents, guardians, and other caregivers.





Schools routinely collect data to inform a range of activities, from basic administration and support services to teacher evaluations, student learning outcomes, and student and school performance. Much of this data is collected through education technology (edtech) tools. These tools allow educators, schools, and districts to more effectively and efficiently deliver instruction, improve student learning and engagement, and measure performance and outcomes.

With the COVID-19 pandemic and the shift to online learning, many schools and districts rapidly adopted new edtech tools to continue teaching students remotely and to assist with return-to-school efforts. Although these tools have provided a quick response to learning needs during the pandemic, it is important to understand the processes by which they collect, use, share, and maintain student data. Without thinking through the ethical and equitable use of student data associated with increased data collection and use, schools and districts may unintentionally put student privacy at risk.

Schools and districts need student data to perform their duties and to better serve students. However, the loss of trust due to insufficient privacy protections and poor communication can impede access through fierce parental opposition, restrictive federal and state regulations, and a general lack of cooperation. By better understanding stakeholder concerns regarding student privacy and adopting good data governance policies and practices, school and district leaders can create a culture where the entire school community works together to support better educational outcomes while protecting student privacy.

This section provides a short overview explaining the concepts of student data, student privacy, and data governance, which are foundational for schools and districts as they seek to implement policies and communicate effectively about student privacy.

What is Student Data?

To understand student privacy, it is important to first establish a common understanding of what student data is and the different kinds of student data that are collected and must be protected. See infographic on next page for additional information.

Student data is student information that is collected and used in the educational context. This 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 a student's devices at home.

This section provides short summaries and examples covering key questions regarding student data, including the purpose, types, and actors involved.

Examples of student data collected throughout a student's educational journey include:¹

- › Name, age, gender, race, ethnicity, socio-economic status, and other demographic data requested or required when registering a student for school at the beginning of the school year;
- › 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;

What is student data?

There are many types of data that support student learning—and they're so much more than test scores. But individual data points don't give the full picture needed to support the incredibly important education goals of parents, students, educators, and policymakers. See the types of data that can come together—under requirements like privacy and security—to form a full picture of student learning. When used effectively, data empowers everyone.

ACADEMIC INFORMATION

- GROWTH
- COURSES
- ENROLLMENT
- GRADES
- COMPLETION
- GRADUATION



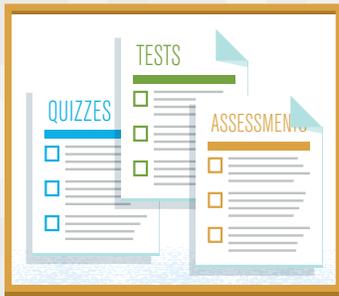
TYPES OF DATA

But what exactly do we mean by student data? Student data is collected from many sources and in many formats, although the type of data, and who can access it, varies.



BY TEACHERS

- OBSERVATION
- ENGAGEMENT



- QUIZZES
 - TESTS
 - INTERIM ASSESSMENTS
 - ANNUAL ASSESSMENTS
- ### TESTING



- ATTENDANCE
 - BEHAVIOR
 - EXTRACURRICULAR ACTIVITIES
 - PROGRAM PARTICIPATION
- ### ACTIONS

- AGE
 - RACE
 - GENDER
 - ECONOMIC STATUS
 - SPECIAL EDUCATION NEEDS
- ### DEMOGRAPHICS



- HOMEWORK
 - LEARNING APPS
- ### BY STUDENTS

REQUIREMENTS

To get that full, clear picture, important requirements must be met for information to be truly useful and to empower people.



AVAILABLE
Data must be there when you need it.



COMPLETE
It must provide a whole picture of student learning.



RELEVANT
Data must be relevant to your needs.



SECURE
It has to be safeguarded, trustworthy.



EFFECTIVE
Educators and policymakers need the skills to use the data.



COMMUNICATE
It must show how students and schools are doing.



SUPPORT
Data should be used to support leaders and educators.



IMPROVE
And data should be used to improve learning.

- › Observational data about a student’s behavior or interests generated by educators throughout the school day; and
- › Student performance, time-on-task, and outcomes generated through homework, learning applications, and standardized tests.

Understanding the different types of student data allows us to better comprehend the sensitivity and potential privacy risks associated with each type, which informs what data schools and districts choose to collect and use and 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 (e.g., a student’s name or identification number) and indirect identifiers (e.g., a student’s date of birth, or other information which can be used to distinguish or trace an individual’s identity either directly or indirectly through linkages with other information).
- › **De-identified data:** Data about individual students that have enough information removed so that a student cannot be identified (e.g., data that has been subjected to statistical techniques to limit disclosure). De-identified data may be published in reports on student achievement or shared with external researchers.
- › **Aggregate data:** Data about groups of students at a summary level (e.g., data shared as part of the school’s federal reporting requirements).
- › **Metadata:** Data that describes and gives information about other data (e.g., indicators on how long a student took to perform on a test as opposed to their actual grade).

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 they are needed;
- › To protect a student’s health and safety, including maintaining medical forms, allergy information, and emergency contact information;
- › To fulfill the basic administrative functions of the school, including collecting, maintaining, and

reporting basic enrollment, attendance, and academic records for a student; and

- › To fulfill the basic administrative functions of local, state, and federal governments, including tracking school and district performance, assessing how funding is being used, and informing the public.

Who Uses Student Data?

Education stakeholders collect and use different types of 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, taking ownership over their educational journey.
- › **Parents** use student data to follow their child’s learning, to partner with educators to provide needed support both at school and at home, and to better advocate for their child.
- › **Teachers** use student data to understand student learning, to tailor lesson plans to individual student success, and to assess student performance and outcomes.
- › **School and District Administrations** use student data to understand the strengths and weaknesses of their educational programs and curricula, to assess what resources they may need to leverage to drive improvements, and to report student performance and outcomes.
- › **State Departments of Education** use student data to measure how schools and districts are meeting 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.

What is Student Privacy?

Privacy is an amorphous concept, defined in different ways by different people in different contexts. 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, their schools, or the government.

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, the word “privacy” has been used as a proxy for talking about fairness and power. For example, institutions, like 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 instance, privacy is not only a definition but plays a role in establishing agreed-upon protections to affirm fairness, including the creation of transparent policies and practices that help correct power imbalances between the individual, the technology, and the institution.

Privacy, as a central component of fairness, often comes up in the educational context. Student privacy refers to the ethical and equitable collection, use, sharing, and maintenance of student data. Why is it so important to protect student data? Any type of data collection, use, or storage 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 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. Privacy can support student success and give them agency over their own information and education.

It is important to keep in mind that privacy is not just another item to be checked off a list to be legally compliant, or a bureaucratic barrier to helping students excel in the classroom. Rather, privacy is integral to the effective use of data to inform priorities and support 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.

When proper student privacy protections are not in place, schools and districts face significant risks to their students or to 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 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 a lack of communication alone can result in a public relations disaster.

To reduce these risks, schools and districts are ultimately responsible not only for ensuring that student privacy is protected but also for practicing transparency and building trust with the school community.

Transparent student privacy policies and practices are necessary to effectively protect privacy in the educational context. In the absence of transparency, students and their parents worry about constant surveillance and monitoring through technological interactions. Among the top student and parent concerns are the creation of a massive permanent record chronicling every time a student has made a mistake; insufficient protection from companies that profit off selling student data or through ads; and impediments to a student’s ability to go to college or have a successful career. Without transparency, it is difficult for parents and students to understand what data is being collected, why it is being collected, and how it is being used. As such, attention to student privacy

and clear communication of privacy policies and practices should be a foundational practice for schools and districts.

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 ensure 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 through 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.²

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.³ The resource includes a checklist for inventorying existing data protection policies and procedures, presenting an opportunity to identify gaps that may be 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.⁴

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 can be 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?

Culture expresses an organization's goals through values and principles. A diverse coalition of national education organizations⁵ created the [Student Data Principles: 10 Foundational Principles for Using and Safeguarding Students' Personal Information](#), which outlines ethical standards by which student data should or should not be used.⁶ As the key responsible party in protecting the privacy and security of student data, school and district leaders should seek to better understand and commit to acting in accordance with these 10 principles.

School and district leaders are key actors in protecting student privacy. However, they are not alone. Each group of education stakeholders has an important role to play to ensure student data is protected and used responsibly.

Schools and districts must work together with educators, parents, and students to create a culture of privacy where all parties understand the need to protect student privacy and act accordingly. Building a culture of privacy requires

an understanding of the legal landscape, a robust data governance program, streamlined vetting of edtech tools, trained educators and staff, and consistent communication.

- › **School and district leaders** should establish robust student privacy policies, procedures, and practices; properly train educators and staff handling student data; and facilitate meaningful communications with parents to protect student privacy. Schools and districts should also consider integrating digital citizenship and literacy into their curriculum to help students develop skills necessary to manage their own privacy and security. Digital citizenship means students understand how to engage ethically online, think critically about the content and resources they view, and embrace a culture of privacy and security to protect their personal information.

Additional Resources:

- [US Department of Education Privacy Technical Assistance Center \(PTAC\): Privacy](#)⁷
 - [PTAC: Transparency Best Practices for Schools and Districts](#)⁸
 - [North Dakota School Boards Association \(NDSBA\): Model: North Dakota Student Education Records Access and Amendment Procedure](#)⁹
 - [PTAC: Checklist for Developing School District Privacy Programs](#)¹⁰
 - [Consortium for School Networking \(CoSN\): Trusted Learning Environment \(TLE\) Seal Program](#)¹¹
- › **Educators** should proactively share information about the purpose and mechanisms of student data collection and use in the classroom with students and their families, and take precautions to ensure the tools they use adequately protect student privacy.

Additional Resources:

- [FPF, ConnectSafely: The Educator's Guide to Student Data Privacy](#)¹²
- [International Society for Technology in Education \(ISTE\), Project Unicorn: Better Edtech Buying for Educators: A Practical Guide](#)¹³
- [Common Sense: Policy Annotator Training — for Educators](#)¹⁴

DEVELOPING A COMMUNICATIONS STRATEGY



The best communications approach is one that is:

- › **Clear:** Speak honestly, directly, consistently, and transparently about student data collection, use, sharing, and maintenance.
- › **Confident:** Demonstrate the value of data in helping students and share successes.
- › **Reciprocal:** Listen to your stakeholders and create space for their voices.

Open and frank conversations about student privacy are necessary to ease the school community's concerns, particularly when children are involved.

Setting Goals

School and district leaders should be thoughtful and intentional about what they are trying to achieve when communicating about privacy protections and responsible data use to both educators and parents. Setting goals for your communications strategy will keep your message clear and consistent. Some potential goals and supporting tactics to consider include:

- › **GOAL:** Building and maintaining credibility and trust
SUPPORTING TACTICS: School and district leadership participation in conferences and seminars around student privacy; the involvement of third-party expert consultants; a demonstrated commitment to a consistent and thoughtful approach to protecting student data; the actions taken to appropriately vet edtech tools used by schools and districts; and regular communications to educators, parents, and students.

- › **GOAL:** Educating about data collection, privacy protections, and data use

SUPPORTING TACTICS: Develop and share an overview of state and federal laws, peer school or district policies, background on how the school or district developed its own policies, and how such policies can be put into practice.

- › **GOAL:** Demonstrating the impact of collected data on educational systems and individual students

SUPPORTING TACTICS: Share examples of state and federal funding shifts; record and amplify educator and student success stories with specific edtech; invite and document parent and educator stories highlighting individual student improvement; and incorporate data and stories into local, state, and federal reporting.

- › **GOAL:** Alleviating concerns about how the school or district is using and protecting student data

SUPPORTING TACTICS: Share detailed background on how the school or district developed its policies; share how the school or district interacts with third-party websites and tools to require adherence to policies; provide presentations by tech experts regarding effective data protection strategies (that the school or district has implemented); and provide a feedback mechanism for educators, parents, and students.

- › **GOAL:** Gaining approval from decision makers on new data-driven approaches

SUPPORTING TACTICS: Demonstrate the need for evaluating and assessing current edtech; encouraging wider adoption of effective edtech with educators, parents, and students; promote

effective at-home edtech activities with parents and students to garner feedback and support; and share success stories from peer schools or districts regarding student achievement and funding increases.

- › **GOAL:** Increasing participation by educators and parents in student privacy learning sessions

SUPPORTING TACTICS: Use existing “captive audience” situations like educator in-service and parent/educator conferences; incentivize attendance at PTA meetings and back-to-school events; hold data-specific educational forums for leaders in both groups to disseminate information back to the larger group (consider hosting those events both on- and off-campus); fund relevant educator professional developments; communicate the prioritization of privacy by the school and district often; and remind educators, students, and parents of their roles and responsibilities as members of a learning community building a culture of privacy.

Creating a Communications Roadmap

Once you have clearly established your communications goals, it is time to develop a roadmap to achieve them. A confident, positive communications posture is key to building long-term trust with stakeholders. When developing an effective communications strategy, school and district leaders should keep the following tenants in mind:

- › **Be proactive.** Establishing open and consistent lines of communication with educators and parents *before* an issue occurs is key to avoiding preventable frustration later on. Don't wait to talk about student privacy until something goes wrong — your audience will not only be upset but will also wonder what else you might not have told them. Repairing trust is challenging.
- › **Be honest and engaged.** Because data collection involves inherent risks and benefits, acknowledge and address concerns upfront. Rather than minimizing educator, parent, and student concerns, proactively describe safeguards in place to diminish and mitigate potential harm. If adequate safeguards are not in place, work with stakeholders to fill the gaps by passing policies, training staff, and/or educating the community. Early reassurance that the

school and district have the child's safety as a top priority can increase parental trust and goodwill, especially as unexpected risks arise.

- › **Be specific.** Articulate how data collection and use can improve teaching and learning and better support students. Use language that is simple and direct for all stakeholders to understand. Providing specific, concrete examples of how and why data is collected and used to help teachers and students can bring to life an otherwise very technical subject.
- › **Be mindful.** Keep in mind that the “data” you are talking about has a face—students—about whom educators and parents care deeply. Try to avoid technical jargon about data and processes and instead emphasize the human element of how data can help real students.
- › **Be humble.** There is often no need to reinvent the wheel. Ask around for help if and when needed; nearby and peer schools and districts have likely faced similar challenges and developed student privacy policies and effective communications materials in response.
- › **Be accountable.** Provide an overview of existing laws and policies that govern the school's, district's, and third-party vendors' responsible use of data. Communicate how offenses are addressed and disciplined, and how educators and parents can hold the school, district, and third-party vendors accountable. Educate parents on their rights when it comes to opting out and providing consent.
- › **Be prepared.** Student privacy concerns can be conflated with other political, social, or technological debates. Be ready to respond to these comments by steering conversations back to student privacy and address broader concerns at the next opportunity.

Communications Best Practices

Privacy, while seemingly straightforward, is a broad term that is frequently used without being properly defined. While some think of privacy as secrecy, others interpret it as confidentiality, security, or safety. Online privacy brings up a host of unique considerations and concerns, and in the digital context, many conflate student privacy with data security. Individual feelings about privacy are often intensely personal and linked to a lack of trust, a power discrepancy, or concerns around fairness.

When communicating about privacy, and particularly student privacy, it is important to consider the multiple perspectives that different audiences bring to the conversation and work to mitigate any concerns clearly and confidently. Below are some recommendations for communicating about student privacy.

Use Clear Language

Conversations about privacy are nuanced and tend to be full of jargon. These complex technical terms, if not defined, can be interpreted differently by different people. Be aware of the terms you use, reduce jargon to improve clarity, and provide context and meaning to increase audience understanding. Below are a few commonly used terms in district and vendor privacy policies that all stakeholders handling student data should understand:

- › **EdTech:** This term refers to a diverse set of online educational programs, websites, and applications used by schools, educators, and students. As this term is broad, it is important to name and define the specific type of technology collecting and using student data; explain the purpose of the technology, the benefits of use, and any potential concerns of that use; share information about mechanisms being taken to address those concerns; and highlight ways to opt in to systems, when appropriate.
- › **Data, Data Use, and Data Sharing:** Schools and districts can mitigate some privacy concerns by devising effective strategies to explain the lifecycle of student data, including collection, use, sharing, and maintenance.
 - Avoid terms with negative connotations like “exploit” or “manipulate” to describe how data is used. General terms like “studying” or “evaluating” are preferred.
 - The term “data sharing” also often negatively connotes that data is given to a third-party or made public without adequate protections. When discussing data sharing, be very specific on the purpose, limitations, and parameters set around the shared data, and the safeguards in place that protect student privacy.
- › **Data Governance:** An organizational approach to data and information management that is formalized as a set of policies and procedures encompassing the

full lifecycle of data, from acquisition to use to disposal. It includes establishing policies, procedures, and standards regarding data security and privacy protection, data access, and data sharing.

- › **Consent:** An agreement to the terms of or permission to move forward with data collection, whether that be related to the use of a student’s picture in the school newspaper or the use of a new edtech tool in the classroom. Parental consent is required for the educator, school, district, or vendor to collect personally identifiable information from the student. Sometimes, consent is described as “informed,” which means parents and students understand the potential consequences of student data collection and use. “Voluntary” or “freely given” consent means parents and students were not coerced into giving consent. In seeking consent, it is important to be clear about the type of consent, the level of confidentiality involved in participation, and specific information given to the individual to gain consent.
- › **School Purpose:** A purpose that is directed by or customarily takes place at the direction of the school, assists in the administration of school activities, or is otherwise for the use and benefit of the school. This includes instruction in the classroom or at home, administrative activities, and collaboration between students, school staff, or parents.
- › **Anonymous:** This term can have different connotations depending on the audience’s level of privacy knowledge. Generally, when speaking with the public, “anonymized data” is data that has been completely stripped of any identifying personal information. “De-identified data” has enough information removed so that an individual student cannot be identified and “aggregate data” combines data from individual students at a summary level.
- › **Profiling:** Any form of automated processing of personal data to evaluate certain personal aspects relating to a natural person, in particular, to analyze or predict aspects concerning that natural person’s performance in school, at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

[Consider Your Audience](#)

When speaking about student privacy, it is important to be specific and tailor your message to your audience. Consider the background and experiences of your audience as you prepare for conversations about student privacy. For example, districts that have many parents who work in technology may approach a conversation differently than those with many parents who are government officials. Further, messaging to educators should look different from messaging to students. Your audience may also raise new considerations and questions, so you should encourage their active participation and keep in mind the value their individual perspectives will bring to the table.

[Communicate to Establish Trust](#)

Providing your audience with proactive, regular, and predictable updates will build trust within your school community. Open communication shows that the school or district is actively seeking to engage educators, parents, and students as partners in its efforts to better protect student privacy. Depending on the culture of your district, certain mediums may be more effective than others. For example, email, in-person meetings, phone calls, or the use of a (pre-vetted) app could be the best way to keep your community in the loop. Schools and districts should employ more than one of these approaches as it can be assumed that the community is diverse with different communication preferences. Through this outreach, invite feedback and encourage participation from your audience to establish a respectful dialogue. Ultimately, parents, educators, and school and district leaders have the students' best interests in mind. Open and constructive dialogue is key to engaging audiences, maintaining trust, and supporting positive outcomes.

[Prioritize Equity and Engage Inclusively](#)

Be mindful that some of your students and their families may face significant barriers when accessing communications about student privacy. Students from marginalized groups who have experienced discrimination are less likely to trust that schools, districts, and edtech companies have their best interests at heart when using student data. Therefore, it should be a priority for school

and district leaders to ensure parents and students from marginalized groups are proactively engaged in conversations about student privacy and that schools and districts are employing different strategies to broaden the reach of their communication efforts, such as:

- › Providing communications across multiple channels to ensure accessibility by all parents, educators, and students. Families who use assistive technologies or with limited access to the internet and devices may face difficulties accessing communications issues solely through digital formats, particularly channels that require high bandwidth.
- › Translating communications into other languages for non-native English speakers. If you are planning convenings, consider including bilingual facilitators or providing translators.

Fairfax County Public Schools (VA) is an example of this practice. Web pages, [including the list of approved tools that require parental consent](#) follow a consistent format and the language is consistent for every school, only the list of applications is different. Automated translation is used on the website, but important documents such as permission forms for consent for certain tools are professionally translated into the official district communication languages.

Find more general advice on effective communication strategies tailored by audience and ways to build trust in our [Nothing to Hide Toolkit](#), developed by the Future of Privacy Forum (FPF) and Actionable Intelligence for Social Policy (AISP) in order to help Integrated Data Systems (IDS) and government leaders engage stakeholders and increase communities' trust in the value of IDS.³⁵

Check out the resources below to find out more about effective communication strategies and tools:

- › [FPF: Effectively Communicating Student Data Privacy to Parents and Communities](#)³⁶
- › [ExcelinEd: Student Data Privacy Communications Toolkit](#)
- › [New Zealand Government: Online Engagement](#)³⁷

CREATING A STUDENT PRIVACY WEBSITE

An easy to navigate website is an essential tool for effectively communicating with your school community — from school principals and administrators to parents, educators, and potential third-party vendors — about your student privacy practices. The school or district, as well as educators, will often point to the website when communicating with various stakeholders, so a well-made central resource should serve all of these audiences.

A website that communicates student privacy well should contain the following information:

- › A link to student privacy or data practices webpage available on the home page
- › A link to student privacy or data practices webpage available in the home page primary navigation menu
- › A copy of or link to the school or district’s annual FERPA notice and/or the rights of parents and students under FERPA
- › A copy of or link to the school or district’s policy regarding student data collection, use, retention, sharing, and protection

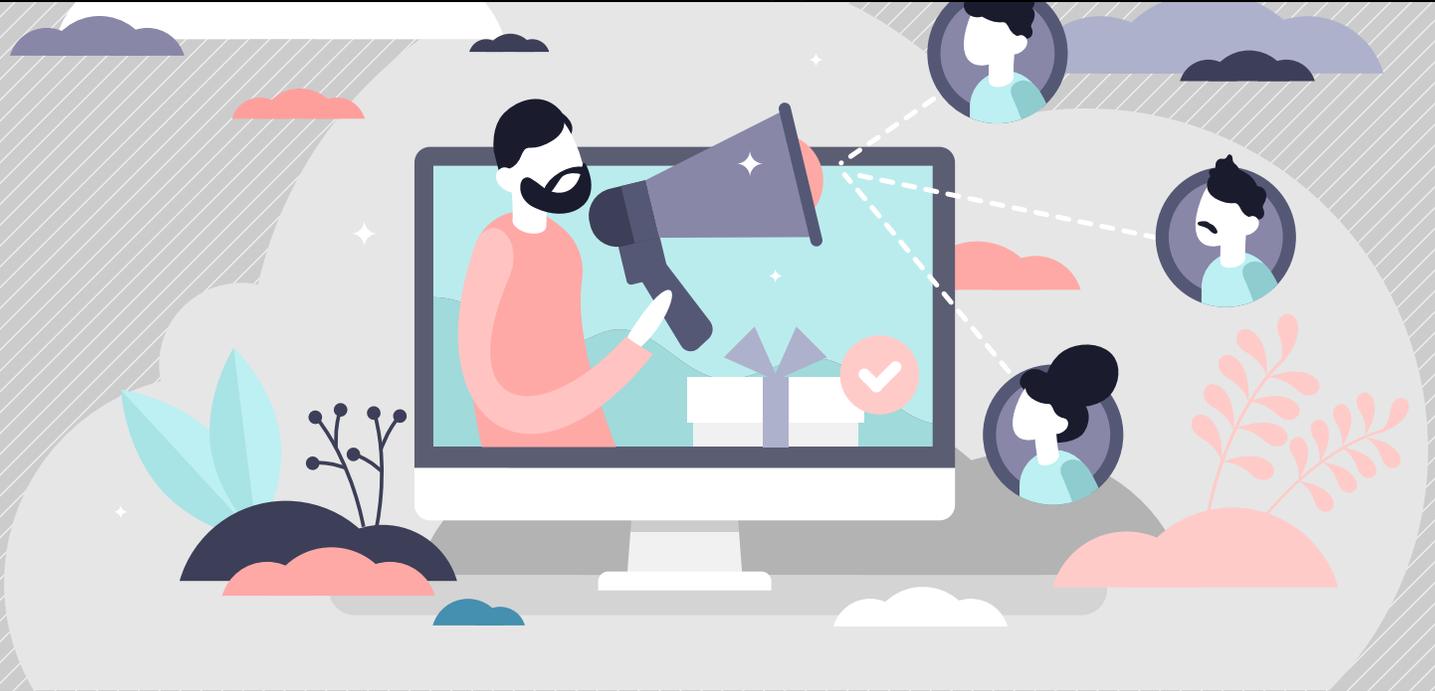
- › A copy of or link to the school or district’s policy regarding directory information
- › A copy of or link to the school or district’s policy under the Protection of Pupil Rights Amendment (PPRA)
- › Information about any applicable state student privacy laws or district policies
- › A list of educational technology tools being used in the school or district, and any information about the process to check those tools for privacy and security protection
- › A contact page or email address if anyone has questions about the school or district’s student privacy policies or practices
- › Resources or trainings for educators and school staff on student privacy
- › Clear, transparent language, including words like “will” and not hedging words like “may” or “might”

While that may sound like a lot, a good student privacy website doesn’t have to be complicated (and shouldn’t be). For example, [Cambridge Public School District \(MA\)](#) has created this effective and user-friendly landing page.



For additional inspiration and guidance, here are other great examples of state and district websites for student privacy that are particularly effective:

- › [Ventura County Office of Education, California](#)³⁸
- › [Denver Public Schools, Colorado](#)³⁹
- › [Fairfax County Public Schools, Virginia](#)⁴⁰
- › [Raytown Quality Schools, Missouri](#)⁴¹
- › [Utah’s Data Gateway Metadata Dictionary](#)⁴²
- › [Wisconsin Department of Public Instruction](#)⁴³



To build and maintain trust, schools and districts, in coordination with educators, should communicate openly and often with parents about their student privacy policies and practices. Parents may still be overwhelmed or skeptical about edtech tools after running into technical problems in the wake of COVID-19-related closures in Spring 2020. School and district leaders should be sympathetic to the concerns of parents and be willing to engage and over-communicate, when needed, to problem solve and dispel confusion.

The transition to online learning has reaffirmed that parents are essential partners in students' educational journeys. As such, schools and districts should seek to inform parents of their rights; effectively communicate school and district student privacy policies, procedures, and practices; and engage parents in the development, implementation, and review of student privacy strategies.

Elevator Speech for Talking with Parents

To kickstart a proactive, positive conversation with parents about the collection and use of their student's personal information, school and district leaders may find the following "elevator speech" useful:

*Our school/district cares deeply about our students and seeks to help them succeed in school and in life. To better understand our students, we collect different types of information, including their demographics, attendance, and grades. Student data can help us monitor performance and appropriately and equitably allocate limited resources. It also informs state and federal policymakers' decisions that affect our schools and students. We commit to protecting student information according to the *Student Data Principles*⁴⁴ and have developed/are actively working towards developing a comprehensive data governance policy addressing how student data is collected, accessed, used, and maintained, available for review on our district website (if applicable). We also prioritize building trust and practicing transparency with the school community. As partners in your child's educational journey, we hope you will continue to engage with us, asking questions, sharing concerns, and keeping us accountable.*

Talking Points to Use with Parents

School and district leaders must communicate clearly with parents to alleviate any system-level concerns regarding student data collection and protection. Below are some frequently asked questions followed by corresponding talking points to help guide a conversation with parents, focused on the ways that schools and districts use and protect student data.

1. Why does the school/district use my child's data?

- › Student data provides important information to support our role in your student's educational journey, so they are prepared to succeed in college, career, and life.
- › Data helps school and district leaders make informed decisions on how to allocate resources and best serve each student.
- › Our school/district can observe and monitor the performance of students/educators/schools and make positive adjustments to address identified needs.

2. How is the school/district protecting my child's data?

- › Our school/district commits to safeguarding student data according to federal and state laws and with ethical and equitable privacy practices in mind.
- › Our school/district has/is developing a comprehensive student privacy policy that outlines who has access to data, how data can be used, and the security mechanisms in place to protect student data.
- › Our school/district complies with all existing federal and state student privacy laws, and we train our staff, faculty, and service providers to ensure they also comply.

3. Who has access to my child's data?

- › Educators, staff members, and third-party service providers are only given access to the specific pieces of data required to do their jobs.
- › If a third-party service provider needs access to limited student data to successfully perform its role with our school/district, our contract includes strict controls and consequences to ensure the protection of student data.

4. How is the school/district using my child's data?

- › Our school/district may use online tools, websites, or applications that collect student data. We carefully vet all tools used in classrooms and ensure compliance with federal and state laws regarding data protection and privacy.

5. Do I, as a parent, have any say in how my child's data is collected, shared, and used?

- › At the beginning of each school year, we provide parents with information about their rights related to their child's data and the ability to opt out of sharing [directory information](#), or sharing information with [military recruiters](#).
- › Additionally, our school/district has a number of tools that collect data and are required for delivering instruction and other services to your child. When we share data with these third-parties, we maintain control through data protection agreements. Sometimes, our school/district will ask for your approval for certain tools that require consent because the tool has met our vetting process, but the vendor does not have the ability to sign a data protection agreement (e.g., students sign up for an account directly), and a list of these specific tools will be provided at the beginning of each school year or as new tools are added.

Parental Rights

Under federal and state student privacy laws, parents have the right to access, review, and amend student data.

The beginning of the school year is a critical time to set clear expectations with parents around ethical and equitable practices for student privacy and online learning for the year ahead. Ideally, parents will hear a coordinated message from both their child's classroom educators and the school or district.

Note: The following letter is designed to be adapted according to your school and/or district policies and practices.

Back-to-School Letter

Dear Parents and Guardians,

Welcome back to [school name]! As we begin the new school year, we wanted to take this opportunity to share with you our student privacy policies and practices to demonstrate our commitment to protecting your child's personal information. You can find our school's/district's student privacy policies and procedures here [link to policies] (if applicable: and our list of approved edtech tools here [link to list]).

Our school/district collects student data including scores on tests and assignments, report card grades, student attendance, demographics, information on special needs, graduation and remediation rates, and disciplinary actions. This data is used to [insert purposes of student data collection, use, and sharing, e.g., determine eligibility for support services, help educators and school leaders understand what factors contribute to student success, and to personalize instruction to improve achievement]. While schools and school districts have always collected student data, the creation, storage, and analysis of this information are now largely conducted digitally.

Our school/district believes that student data should be used as a tool to improve student learning and success by informing, engaging, and empowering students, parents, educators, and policymakers. We believe that limited student data should only be shared for a legitimate educational purpose and that there should be clear, publicly available rules and guidelines for how student data is collected, used, safeguarded, and destroyed.

[If applicable: Our district's student privacy policy details the strict procedures and security mechanisms in place to protect digital student data and is available for you to review here: [link to policy]. The policy ensures only authorized individuals with a legitimate educational interest can access personally identifiable information about your child in order to successfully fulfill their responsibilities.]

In addition to data the school/district collects, your child's educator(s) may use online learning tools and applications that also collect and use data. Please be aware that federal laws like the Family Educational Rights and Privacy Act (FERPA) and state laws protect student privacy and give parents certain rights related to their child's data. [If applicable: We carefully vet all tools and applications used in the classroom, and they must comply with federal student privacy laws governing data collection, use, and maintenance. You may be asked to sign a consent form for your child to use certain tools if we are unable to verify that the tool meets our student privacy obligations.] [If applicable: Educators are only allowed to use education technology tools with students when that edtech company has signed a privacy-protective contract with our district or the educator has gotten your written consent for an approved tool that lacks a contract, which is often the case for many free tools.]

[If applicable: We encourage you to review our district's student privacy policy online at [insert url] to understand how we work to keep your student's data and their privacy protected.] We also encourage you to do the same with technologies you use or are considering to assist with your child's learning. To aid you with vetting privacy policies and understanding use of your student's data, [The Common Sense Privacy Program](#) provides expert evaluations of edtech tools' privacy policies to assess the websites and online tools of many of the tools we use, as well as others you may be considering using with your student.⁴⁵

If you have any questions or concerns, please visit [insert url] or contact the district's [insert party responsible for student privacy, e.g., Chief Information Officer] [insert name] at [insert email/phone number].

Thank you and we look forward to a successful school year.

Kind Regards,

[insert signature]

Educational Technology Consent Form

Each year, schools and districts should provide notice to parents and guardians regarding student use of various edtech tools and platforms. Take this opportunity to clearly communicate the platforms students will be using, their educational value, and the precautions that the school is taking to safeguard student information against the privacy risks that may come with the use of any app or online tool. The consent must be for specific tools, and cannot be a broad permission to share data with any approved third-party.

Note: The following form is designed to be adapted according to your school and/or district policies and practices.

Educational Technology Consent Form

Dear Parents and Guardians,

Below is a list of online learning tools that one or more of your student’s educator(s) plan to use to deliver instructional materials and enhance your child’s education at [school name]. In the interest of transparency and to ensure you are informed about the district’s use of these resources, we wanted you to be aware of what they are, how they will be used in your child’s classroom(s), and how any information collected from these programs will be appropriately used and safeguarded.

[Optional language: Since our district was unable to verify some of these tools were compliant with our student privacy legal obligations, the Family Education Rights and Privacy Act (FERPA) requires your consent for the use of the tools below that collect information included in your student’s education records or other information that could be personally identifiable to your student (including, but not limited to, name and age).]

[Optional language: Under [insert state] law, our school/district is also required to [insert description and requirements], e.g., Under Colorado’s student privacy law, schools are required to list the apps and programs students use in the classroom. (C.R.S. § 22-16-107), Under New York’s student privacy law and accompanying regulations, both edtech companies and schools are required to comply with the NIST Cybersecurity Framework. (8 NYCRR part 121).]

Website or Online Tool	Brief Summary of Educational Purpose/Use	Link to Privacy Policy or Terms and Conditions

Please take a moment to review the websites and online tools we plan to use, as well as what personal information the site collects on each terms of service. Some resources that may help you in making this decision are listed below:

- [Common Sense Privacy Program](#) provides expert evaluations of edtech tools’ privacy policies to assess the websites and online tools listed above as well as others you may be considering using with your student.⁴⁶
- For edtech tools not yet reviewed by the Common Sense Privacy Program, try [PriBot](#), a chat bot that uses artificial intelligence (AI) to simplify complex privacy policies.⁴⁷
- Another useful tool is [ToS:DR](#) (Terms of Service; Didn’t Read), which rates and labels online services’ terms of service and privacy policies on a scale from A to E.⁴⁸

If you have any questions or concerns, please visit [insert url] or contact the district’s [insert party responsible for student privacy, e.g., Chief Information Officer] [insert name] at [insert email/phone number].

After reviewing, please sign to acknowledge that you have reviewed and understand the district’s policies and practices with respect to your student’s access to online educational resources, and that you have been provided with access to each online resource provider’s terms and conditions of service. Please return this form to [school name] by [date]. [Optional language: This serves as your permission for your student to have access to the above-listed sites and tools as well as your permission for us to upload your student’s necessary information into the application(s).]

Sincerely,

[Name]

[Title]

Student’s Name: _____

[Optional language: Student ID:]

Parent Signature: _____ Date: _____

Online Learning: Monitoring Attendance and Student Engagement

Online classrooms complicate the once simple process of marking attendance and assessing student engagement. In a physical classroom, a student’s presence is clearly visible and serves as a noncontroversial measure of attendance, while in an online classroom, attendance is much more nuanced and difficult to calculate. Teachers may require students to have their video on to determine presence in class or may check if the student has logged in to a particular website that day. Student engagement and participation also become more difficult to capture in an online setting. Some schools and districts plan to rely on learning analytics, such as tracking the minutes spent logged into a particular website, to assess engagement and participation. Schools should have a solid technical understanding of how they are measuring logins before proceeding down this path, as this can differ between applications and between web and mobile versions of the same tool.

In an online setting, it is justifiable that teachers and schools are turning to new tools and types of measurements, but this also means schools and teachers must set baseline expectations for parents and students. This communication should provide students and families with the details of how students will be assessed, including the types of information collected and how it will be used, particularly any effects on grades or student records, and provide them with opportunities to request accommodations or alternatives.

Note: The following form is designed to be adapted according to your school and/or district policies and practices.

Sample Parental Notice

Dear Parent or Guardian,

Your child’s attendance, participation, and engagement are all important factors that our school has always monitored and measured. However, as a result of our transition to an online learning environment, how we do this will now look different. We would like to share with you how attendance and participation and engagement will be monitored and tracked in an online setting, including the types of information that will be collected and how it will be used.

Your child’s attendance will be measured by [insert the types of data that will be used to measure presence in class].

Your child’s participation and engagement will be measured by [insert how participation and engagement will be measured, including the types of information collected, the method of measuring, and how it will factor into student grades].

If you believe the information we have listed above will not be an accurate portrayal of either your child’s attendance or participation and engagement, please reach out to [school staff member] to request an accommodation or alternative. We know that everyone’s home learning environments look different, and we want to make sure that we’re providing your child with every opportunity to succeed during this time.

Online Learning: Behavioral, Social, and Emotional Learning Surveys

As some schools and districts consider administering social, emotional, and behavioral screening surveys, it is important to consider the privacy and equity concerns and requirements. Under the Protection of Pupil Rights Amendment (PPRA), whether schools must obtain **opt-in or opt-out parental consent prior to administering screeners depends on a number of factors shown below.**

Student participation required	Covers eight protected categories	Opt in/Opt out
Yes	Yes	Provide notice and parents must opt in for the student to take the survey
Yes	No	Provide notice and parents have the right to opt out
No	Yes	Provide notice and parents have the right to opt out (but check your specific state law first)
No	No	Provide notice only if the survey was created by a third party. In that case, parents have the right to opt out.

For more information on PPRA, see [FAQs: The Protection of Pupil Rights Amendment](#).⁴⁹

If your school or district determines that administering social, emotional, and behavioral screeners are necessary in order to assess the impact of the COVID-19 pandemic and national events related to systemic racism on student wellbeing, be sure to notify parents and guardians of their rights, explain the purpose of the survey, describe what student data will be collected, and detail potential follow-up measures based on the results.

Note: The following form is designed to be adapted according to your school and/or district policies and practices.

Consent Form

Our school will be administering a social, emotional, and behavioral screener to assess the impact of the COVID-19 pandemic, shift to distance learning, and national events related to systemic racism on student wellbeing. The data that will be collected will include screening results and personal information, such as age, gender, and race/ethnicity. All information will be kept confidential and in accordance with student safeguards defined by the Family Educational Rights and Privacy Act (FERPA). Your permission is required, pursuant to the Protection of Pupil Rights Amendment (PPRA), to begin the screening process. You also have the right to inspect, upon request, the screening instrument and any questionnaires before they are administered or distributed to your child. You may choose to allow your child to be administered a screener or not and may choose to withdraw your permission at any time. For the purpose of administering the social, emotional, and behavioral screener, data collection is defined as [insert data collected, e.g., questionnaires and interviews with your student's teachers or other educators]. Your agreement to participate or your refusal to participate in the screening and/or data collection will in no way affect the services your student receives at [school name].

As part of the social, emotional, and behavioral screening and referral process, your child might be asked to complete questionnaires and interviews by qualified professionals, or the school staff will complete a screener to identify any social, emotional, or behavioral issues. If social, emotional, or behavioral needs are identified, you will be notified by the school. You must give informed written permission before your child may be provided social, emotional, or behavioral services through the school. If necessary, the school will also link you and your student to external behavioral health services in the area.

[Optional language: If your child is involved in the criminal justice system, the court may require us to report to it about his/her participation or progress with consequences if he/she does not follow the court requirement.] If you do not wish for your student to receive social, emotional, and behavioral support services, you have the right to withdraw him/her from the services without penalty, at any time.

Permission to Participate in Social, Emotional, and Behavioral Screener and Data Collection

Date: _____ School: _____

Student Name: _____

By my signature below, I am confirming that I have read the document and have been informed of my rights under PPRA and FERPA.

Please check the appropriate statement, sign and return this form to the school as soon as possible to [staff name/office/department].

- I give permission for my child to participate in the universal social, emotional, and behavioral screening process and data collection.
- I do not give permission for my child to participate in the universal social, emotional, and behavioral screening process.
- I understand that I will be notified and will be required to provide written informed consent prior to any intervention or other social, emotional, and behavioral services are provided for my child.

Signature of Parent(s)/Guardian(s): _____

Date: _____

The example above was adapted from the [Louisiana Department of Education Parental Consent Form for Universal Social, Emotional and Behavior Screener](#).

Parents as Partners in Protecting Student Privacy

Parents, especially those new to educational settings, may be unaware of what data is collected about their child and how that data is used and protected by educators, staff, and school and district administrators. Further, in an effort to assist their child in learning, parents may unwittingly use online edtech that puts their child's privacy at risk. To help parents understand the importance of protecting student privacy and encourage their participation in cultivating a culture of privacy, schools and districts may wish to consider sharing a tailored version of the following letter with parents:

Note: The following form is designed to be adapted according to your school and/or district policies and practices.

Sample Parent Letter

Dear Parents,

As educators, the protection of our students' privacy is not only paramount but also mandated through state and federal law, like the Family Educational Rights and Privacy Act (FERPA). As explained in our back-to-school letter, under FERPA, we and our technology providers are responsible for protecting student data, including data that is collected through digital formats, like learning applications and technologies. As such, our district only uses and only approves the use by teachers and students in the classroom of technologies and applications that adhere to strict data protection procedures and security [[link to school or district privacy policy here](#)]. Doing so helps ensure only authorized individuals with a legitimate educational interest can access personally identifiable information about your child in order to successfully fulfill their responsibilities. This also ensures that the technologies used align with privacy standards, class curricula, and learning outcomes.

Given the breadth of learning applications and technologies available online, you or your child may be interested in using these kinds of tools to assist with classwork and learning. However, if these tools have not been vetted in a similar manner to our district's vetting process, you may be putting your child's and your own privacy at risk. Among these risks are:

- Age-inappropriate content or content misaligned with learning standards;
- Unmoderated or inappropriately moderated activities and discussions;
- Sharing of your child's data (or any data on your family's devices) to unidentified third parties;
- Targeted marketing and advertising to your child;
- Introduction of malware or viruses to your computer;
- Creation of data profiles based on student data and online interactions; and
- Increased potential for cyberbullying and surveillance of your child.

To limit potential privacy violations, we encourage you to review our district's student privacy policy here [[insert link](#)] and to do the same with technologies you use or are considering to assist with your child's learning. To aid you in vetting privacy policies and understanding the potential uses of your child's data, the [Common Sense Privacy Program](#) provides expert evaluations of edtech tools' privacy policies to assess the websites and online tools of many of the tools we use, as well as others you may be considering using with your child⁵⁰

Thank you for continuing to be collaborative partners in your child's learning and privacy protection. As always, should you have any questions about our policies or ways to improve privacy for your student at home and online, please contact us.

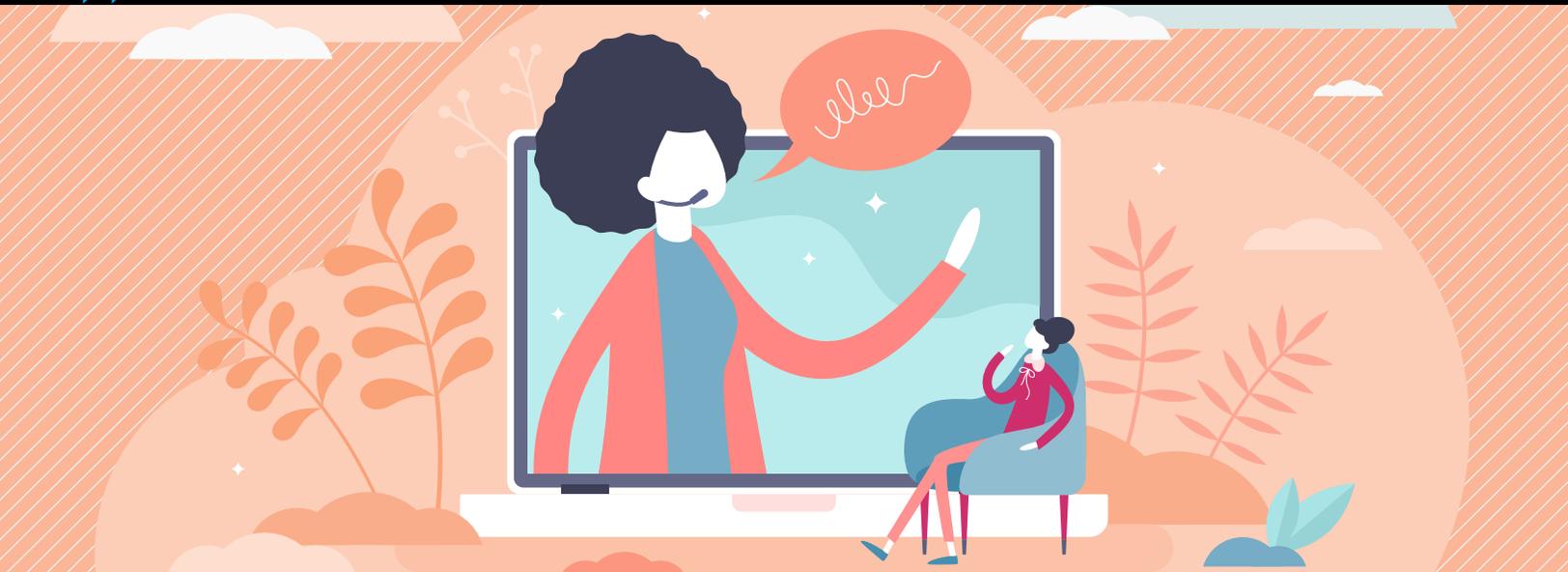
Sample Text Messages to Parents

Back-to-School Text

From the school/district: [[School/District Name](#)] Families, Remember to sign the educational technology consent form and review our student privacy policy — together, we can protect student privacy: [[add link to privacy information here](#)].

General Follow-Up Text

From the school/district: [[School/District Name](#)] Families, Read how we are working together to protect student privacy: [[add link to privacy information here](#)].



From selecting privacy-protective edtech tools to teaching students about digital citizenship, educators play an essential role in protecting student privacy. They are also critical in building parent trust in and understanding of the role of technology in the classroom to create a culture of privacy in school communities. While educators may have the best intentions, without proper training and support from schools and districts on student privacy, student data may be unwittingly put at risk. Schools and districts should recognize educators as the first line of defense in safeguarding student privacy and provide clear and easily accessible guidance describing the educator’s role and responsibilities, the school or district student privacy policies and procedures, legal requirements, and ethical and equitable practices.

Elevator Speech for Talking with Educators

The following “elevator speech” is designed to help school and district leaders start a dialogue with classroom educators about the importance of protecting student privacy and using only school- and district-vetted edtech tools in their classrooms.

As educators, you are constantly seeking the best tools to help your students learn and thrive. Useful websites, apps, and other tools are readily available to assist you in monitoring student progress and improving student learning. While these tools are easily accessible and tempting to download, I’d ask that you pause and check with [the school IT department/privacy officer] first. We don’t want to prevent you from finding new tools to better support your students, but to protect student privacy we must ensure that anything you use in your classroom complies with state and federal student privacy laws, as well as our district’s student privacy policy. [If applicable: The good news is that we have already vetted several great apps that do meet all of those requirements, which you can access here [link to list].] If there is an app that you would like to use that has not yet been vetted by our IT department, let us know so that we can consider it in future evaluations for use in classes. You are also on the frontlines of communicating with students and parents about the importance of student privacy and our school/district policies and practices. Familiarize yourself with the [Student Data Principles](#)⁵¹ and the ways our school/district works to protect student privacy to build trust with parents and students, allowing us to use student data and edtech tools to better serve our students.

Talking Points to Use with Educators

Educators are typically the first point of contact for parents with questions or frustrations concerning educational technologies. It is extremely important that educators feel prepared to address any privacy-related issues with parents and are well-informed regarding student data collection, use, and protection. Additionally, educators must be aware of the school's/district's approval process to vet and confirm use of online tools for their classrooms; otherwise, they may download and use something that is not privacy-protective. Below are some frequently asked questions followed by talking points to adapt and use with educators to ensure they have a high level of comfort regarding student data policies.

1. Does the school or district have a policy around student privacy?

- › *Our school and district collects various amounts of student data and has a comprehensive privacy policy in place to help keep data safe. You—along with any parents that may have questions—can access that policy at any time by _____ . If you have questions or need clarification regarding this policy, please contact _____ .*
- › *Ensuring student safety and privacy is the right thing to do and part of our obligation as educators/school staff. There are serious consequences if these policies are not followed — the entire district/school could lose public trust and face other repercussions, such as costly lawsuits.*

2. What are my responsibilities in protecting student data?

- › *As an educator, you have access to some student data necessary for monitoring student progress and creating individualized learning plans. This means you are responsible for ensuring that it is not lost, accessed, or shared without proper authorization. If you have any questions about how data can or should be best used and protected, let us know and we're happy to help. Additional resources are available at _____ .*

3. What do I do when I want to adopt a new educational technology tool?

- › *Our district has developed a vetting process for you to get applications approved prior to bringing them into the classroom. Find our policy here _____ . These policies are not*

meant to limit creativity or infringe on your professional perspective, rather they are in place to help ensure the safety and privacy of you and your students.

- › *In addition to our vetting and assessments, you may choose to refer to a resource like the Common Sense Privacy Program, which provides expert evaluations of edtech tools' privacy policies, to assess our school/district's pre-approved websites and online tools as well as any others you may be considering using in your classroom.⁵²*

4. What are the rules around posting about my students online?

- › *Be careful posting any information about your students online. While posting a picture on Facebook, Instagram, Twitter, TikTok, or another social media platform may seem harmless, this may inadvertently subject students to cyberbullying or reveal sensitive information, such as their whereabouts, to unwanted parties.*

Evaluating Edtech Tools

Even before the transition to online learning, edtech tools had become indispensable to our K-12 education system. Schools and districts rely on dozens, if not hundreds, of third-party partners to enhance teaching and learning. Data gathered⁵³ by LearnPlatform⁵⁴ indicated that “1,327 ed-tech tools were accessed on average each month after the coronavirus-related closures. That’s a nearly 90 percent increase over the previous monthly average for the 2018-2019 academic year, when just 703, were accessed.” As part of a robust data governance program, schools and districts should have a process in place to vet edtech tools, regularly inventory all of the tools used within their school/district, and practice transparency by making a list of pre-vetted tools and tools currently in use available to educators, parents, and students.

The US Department of Education recommends that “schools and districts should be clear with both teachers and administrators about how proposed online educational services can be approved, and who has the authority to enter into agreements with providers;” this includes free services.⁵⁵ If your school or district has not yet established a vetting and review process for edtech tools, school and district leaders should ensure that educators are equipped to evaluate the new educational technologies they bring

into the classroom for legal compliance and other important student privacy protections. Educators should receive training on federal and state legal obligations and the school's or district's student privacy protection commitments, summarized below:

Federal Legal Requirements. Schools and districts should inform educators of the legal requirements under the Family Educational Rights and Privacy Act (FERPA) and Children's Online Privacy Protection Rule (COPPA).

- › FERPA, which applies to all schools receiving funding from the US Department of Education, guarantees parents access to their children's education records and restricts the parties to whom schools can disclose students' education records without consent. Educators should know that under FERPA, schools are required to obtain parental consent to share information in a student's education records, which is the case for most edtech tools, or qualify for an exception. Most edtech providers receive student information under the "school official" exception, which requires schools to ensure the edtech company is doing something for which the school would otherwise use internal staff; has a legitimate interest; is under direct control of the school; and any data is only collected, used, and shared for the original purpose it was collected for.
- › COPPA, which applies to operators of commercial websites and online services, regulates collection of information from children under the age of 13. Educators and other school officials, such as district administrators, are authorized to provide consent on behalf of parents for the use of online tools in the context of educational programs. Educators need to know that for this age group, COPPA requires that student information is used solely for a specific educational purpose and not for commercial purposes.

Commitments. It is also important for educators to consider key questions that are vital in upholding certain student privacy protections. For example, educators should check to see if the vendor creates a profile of students for non-educational purposes or if any advertisements are shown to students while using the product. The list of questions below should be provided to educators to aid in their vetting process.

Evaluating Edtech Tools for Privacy Checklist

- › Does the app collect personally identifiable information (PII)?
- › What other types of data are being collected? (de-identified data, aggregate data, metadata?)
- › Does the vendor commit to not further share student information other than as needed to provide the educational product or service (such as third-party cloud storage, or a subcontractor the vendor works with under contract)?
Tip: The vendor should clearly promise never to sell student data.
- › Does the vendor create a profile of students, other than for the educational purposes specified?
Tip: When schools share student data under FERPA's "school official" exception, vendors are not allowed to create a student profile for any reason outside of the authorized educational purpose.
- › When you cancel the account or delete the app, will the vendor delete all the student data that has been provided or created?
- › Does the product show advertisements to student users?
Tip: Many states ban targeted ads based on data about students or behavioral ads that are based on tracking a student across the web. Look for a triangle "i" symbol [], an industry label indicating that a site allows behaviorally targeted advertising. These are never acceptable for school use. This is particularly important when evaluating non-education-specific sites or services.
- › Does the vendor allow parents to access data it holds about students or enable schools to access data so the school can provide the data to parents in compliance with FERPA?
Tip: This is one of the criteria the FTC lists as required for a school to be able to provide consent on behalf of a parent.⁵⁶
- › Does the vendor promise that it provides appropriate security for the data it collects?
Tip: A particularly secure product will specify that it uses encryption when it stores and transmits student information. Encrypting the data adds a critical layer of protection for student information and indicates a higher level of security.
- › Does the vendor claim that it can change its privacy policy without notice at any time?
Tip: This is a red flag— current FTC rules require

that companies provide notice to users when their privacy policies change in a significant or “material” way and companies must obtain new consent from users for collection and use of their data.

- › Does the vendor state that the school is responsible for complying with the Children’s Online Privacy Protection Act (COPPA)?
Tip: The FTC prohibits vendors from pushing COPPA compliance onto schools.⁵⁷
- › Does the vendor say that if the company is sold, the service to the school or district is terminated?
Tip: The policy or contract should state that any sale or merger will require the new company to adhere to the same protections.
- › Does the vendor provide notice and indemnify the school or district to take responsibility in the event it or one of its subcontractors experiences a data breach?
Tip: Some states have laws that require schools to notify parents when student data is breached.

The information provided here is only a starting point for training teachers to vet any edtech tools they would like to use in the classroom. Educators will need thorough training to learn these terms and concepts, which are most likely new to them, and learn the nuances of the applicable federal legislation. Here are more resources for providing edtech privacy vetting training to teachers:

- › [FPF: Adopting EdTech: Privacy Vetting⁵⁸](#)
- › [US Department of Education Privacy Technical Assistance Center \(PTAC\): Protecting Student Privacy While Using Online Educational Services: Model Terms of Service⁵⁹](#)
- › [Common Sense: Privacy Evaluations⁶⁰](#)
- › [Consortium for School Networking \(CoSN\): Vetting Online Tools⁶¹](#)
- › [FPF: Student Privacy Pledge⁶²](#)
- › [Ventura County Office of Education: Teacher Flowchart: Student Data Privacy Check List⁶³](#)

Note: The following form is designed to be adapted according to your school and/or district policies and practices.

Email Template to Educators

From: ouremail@schooldistrict.com
Date: December 10, 2020 at 2:13:38 PM CST
To: youremail@gmail.com
Subject: Vetting Edtech Tools!

Dear Educators,

With the start of the school year, you may be exploring new edtech tools to bring into the classroom. While we are excited to see what you have found and encourage you to be creative, it is important for us to make sure that each tool students use is both safe and privacy-protective. We have developed a comprehensive vetting process that can be found here [\[insert url\]](#). We also have a list of applications that have already been approved by the school/district available here [\[insert url\]](#). In addition, there are external educational technology vetting resources that may give you an idea of whether or not the application you’re interested in is safe. For example, check out applications that have been approved by [Common Sense Media’s Privacy Evaluations⁶⁴](#). Remember that you may not use a new application without approval from the school/district. If you have any questions about this process or a particular technology, or if there is an edtech tool you would like us to assess and vet, please contact our [\[school/district staff member\]](#) here [\[insert contact information\]](#).

Practice Privacy When Using Edtech with Students

Selecting safe and approved tools is an important part of protecting student privacy. Teachers also protect student privacy in the choices they make when using these tools.

Recording Video Classes

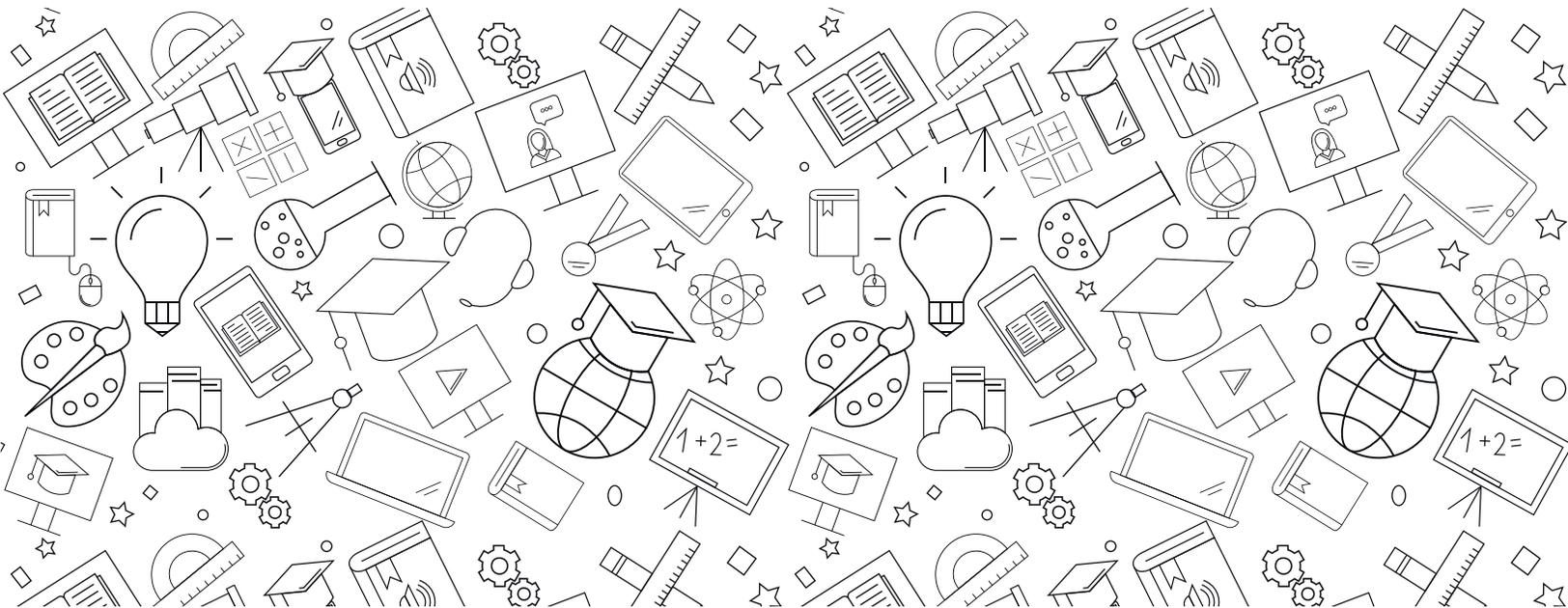
Schools and districts should train educators so they are equipped to protect student privacy before recording video classes. It is permissible for a lesson to be recorded so long as no FERPA-protected student information is disclosed in the recording. Schools and districts should consider creating a process for obtaining parental consent to record video classes if a student's personal information, including their name, likeness, or voice, is part of the recording, and consider developing guidelines for teachers that specify processes for creating, storing, sharing, and deleting classroom recordings in a secure, privacy-protective manner.

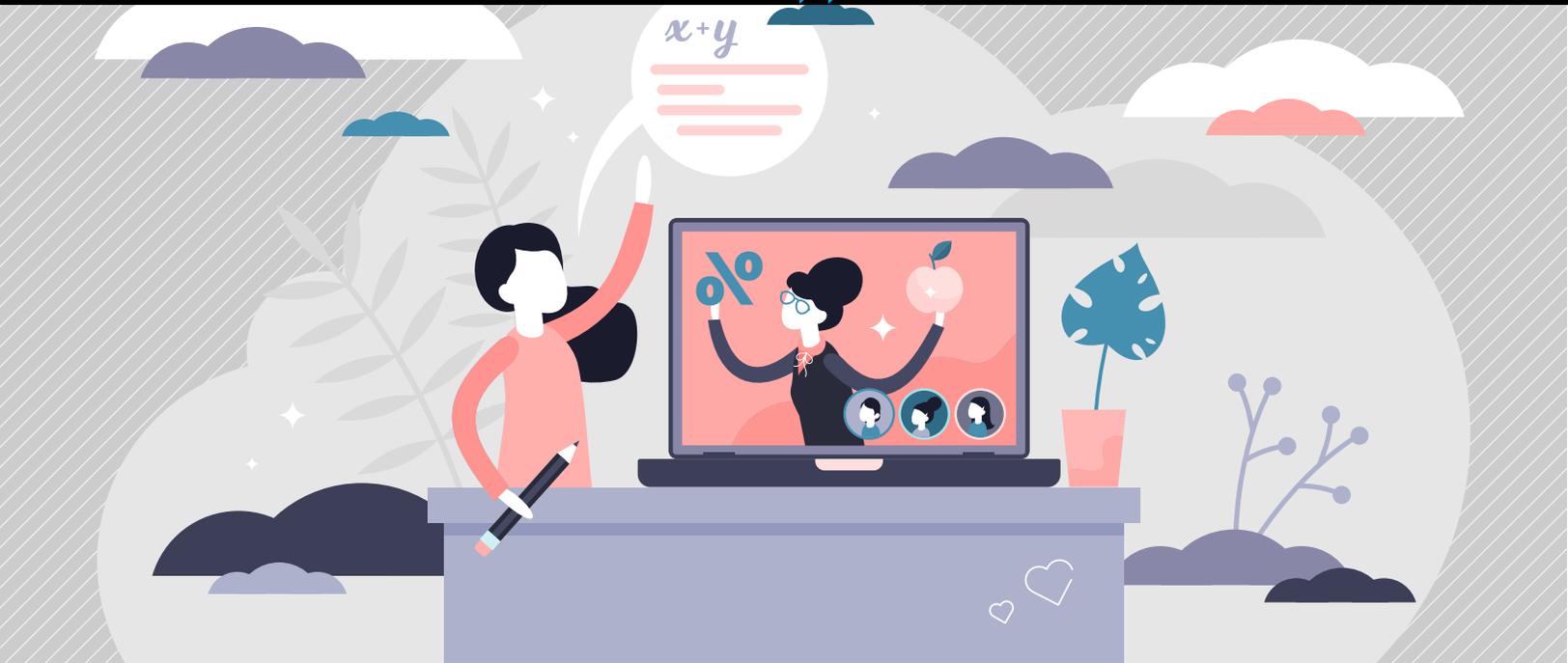
When an educator reaches out about recording a video classroom, encourage them to:

- › Only record the educator's portion of the presentation or lesson, without showing students or recording student participants.
- › Be transparent with students and their parents about classroom recordings. Students should be aware that their lessons are recorded, how long these recordings are stored, who has access to the recordings, and what rights students have to opt-out of attending a live recording.
- › Develop rules of engagement for their online classroom and set standards for how students are expected to participate when a class is recorded.

To find out more about protecting student privacy with video classrooms, see the resources below:

- › [PTAC: FERPA and Virtual Learning During COVID-19 \(Webinar Recording\)](#)⁶⁵
- › [PTAC: FAQs on Photos and Videos under FERPA](#)⁶⁶
- › [CoSN: Video Conferencing Tools in the Age of Remote Learning: Privacy Considerations for New Technologies](#)⁶⁷
- › [Center for Democracy and Technology \(CDT\): Protecting Students in Virtual Classrooms: Considerations for Educators](#)





As students increasingly live and learn in digital environments, they must be empowered to recognize the opportunities and risks of being online, as well as their rights and responsibilities in that space. In addition to educators and parents, schools and districts have an important role to play in developing students' digital citizenship skills and privacy knowledge. While school and district leaders work less directly with students on a day-to-day basis, they still have meaningful opportunities to communicate with students. Whether through policy development, presentations at school events, or during one-on-one conversations, leaders should actively engage students in talking about and practicing appropriate online behaviors that protect their privacy and the privacy of their learning communities.

To include students as active participants in building a culture of privacy, schools and districts should be transparent about data governance and student privacy policies and procedures. This includes transparent communication about any monitoring, filtering, or blocking of online content and activities by the school or district, as well as expectations of appropriate use of technologies by students. In this way, transparent privacy policies and standards that outline when, why, and how

students are monitored and how their data and school technologies are used to support student learning bolsters trust. This trust extends to the technologies used by schools and districts; the policies and practices that govern the use of these technologies; and the intent of teachers, schools, and districts in using technologies that keep students safe online and do not leave them feeling under constant surveillance.

Too often students are excluded from conversations about student privacy. At a minimum, schools and districts should include information about privacy in student rights and responsibilities handbooks or paperwork that may be sent home at the beginning of the year as a way to begin conversations about privacy among educators, parents, and students. However, communications with students should also be designed in a manner that is suitable for each age group. For example, schools and districts may choose to share responsible use of technology policies with elementary school-aged students through animated videos as opposed to a written form. You can find more information on tailoring messaging to the age of a child under the [transparency standard⁶⁸](#) of the [UK's Age Appropriate Design Code⁶⁹](#).

Elevator Speech for Talking to Students

You may choose to adapt this short “elevator speech” when talking to your students about how their data may be collected, used, shared, and maintained. Student buy-in is essential in creating a culture of privacy, and schools and districts can empower students by helping them develop skills to effectively manage their own privacy and security.

Our school/district cares deeply about protecting your privacy. Some of your personal information like your name, age, and grades are needed by the school or district for basic administrative purposes and to help you on your educational journey. We work closely with your parents and teachers to make sure our policies and procedures prioritize safeguarding your personal information. However, you can also play an active role in protecting your own privacy and security by developing your digital citizenship skills and taking proper cybersecurity precautions. This includes learning how to manage your digital identity and reputation; engaging in positive, safe, legal, and ethical behavior online; and being aware of how your data is collected and used.

To learn more about digital citizenship and cybersecurity for students, refer to the resources below:

- › [International Society for Technology in Education \(ISTE\): Standards for Students](#)⁷⁰
- › [Common Sense: Digital Citizenship Curriculum](#)⁷¹
- › [Canadian Civil Liberties Association \(CCLA\): Peer Privacy Protector Project \(PPPP\)](#)⁷²
- › [Google: Be Internet Awesome](#)⁷³

Guiding Questions for Use with Students

Students may engage in behaviors that place their own privacy or the privacy of others at risk. For instance, students may share screenshots or recordings from online classes on social media without the permission of their teachers and peers. When responding to such incidents, school and district leaders can use the following questions to guide a conversation about the need to respect and protect privacy and security. These questions should be adapted as appropriate based on the student’s age and stage of development.

- › What does privacy mean to you? What about security?
- › Why should you care about privacy and security?
- › How might you or others be put at risk when privacy and security are not respected and protected?
- › What are some steps you can take to protect your own privacy and the privacy of others?

Responsible Use of Technology Policy

One way to reduce the likelihood of students engaging in activities that compromise privacy and security is to set common expectations for online activities and behaviors through a responsible or acceptable use of technology policy. Your school or district should solicit input from educators, parents, and students when shaping a responsible use policy to identify shared values and address potential violations.

The example below was adapted from [Montgomery County Public Schools' Responsible Use of Technology Student Expectations](#)⁷⁴ and [Brandon-Evansville Public Schools' Responsible Technology Use Policy for Students](#).

Note: The following form is designed to be adapted according to your school and/or district policies and practices, as well as student age and grade level.

Sample Responsible Use of Technology Policy

Dear Student,

All [school/district name] students are responsible for their own actions and activities involving school/district devices, networks, and systems, and for their files, accounts, and passwords. Based on the responsible use guidelines outlined in this document, you may face consequences if these terms are violated.

Responsible use of technology means engaging with technology safely, respectfully, and ethically (understanding right from wrong). As a responsible user of technology:

I take steps to protect my personal information.

- I keep my usernames and passwords private.
- I keep my documents and other electronic data secure.
- I review privacy policies with my parents before downloading new apps or technology.

I respect and take care of the technology I have access to.

- I do my best to keep the technology in my possession safe and secure.
- I don't make changes to technology equipment or settings that may be harmful.
- I only use school-approved apps on school-owned computers and technology.
- I don't download any apps on school-owned computers and technology.

I use technology ethically.

- I respect the digital privacy of others.
- My use of technology does not put myself or others at risk.
- I comply with software licensing agreements and copyright and fair use laws.

I use technology for educational purposes.

- I avoid online resources that are inappropriate, offensive, or illegal.
- If I see inappropriate material online, I report it in a timely fashion.

I, [student name], understand that it is my responsibility to honor the Responsible Use of Technology Policy. I understand that my actions can affect others and that I will be held accountable for my behavior. I will not engage in activities that are in violation of the Responsible Use of Technology Policy.

I have read the Responsible Use of Technology Policy and agree to these rules and guidelines.

Student's Name: _____

Online Learning: Monitoring Attendance and Student Engagement

Monitoring student attendance and engagement in person was relatively straightforward through physical observations in traditional classrooms. However, with online or hybrid learning environments where such constant physical observation is not possible, schools, districts, and educators have been seeking innovative solutions to ensure students are present, engaged, and learning. With the adoption of new methods for tracking attendance and engagement, students should be informed of the school's or district's policies and be provided an opportunity to ask questions and request alternative strategies.

Sample Student Notice

Dear Student,

As you can imagine, the way we work together in an online classroom will look very different from how we used to work together in person. As a result of our transition to an online learning environment, we want to keep you updated on how we will be taking attendance and measuring your engagement:

- Your attendance will be taken by [insert method for measuring attendance].
- Your behavior will be assessed by the way you interact with your peers and teacher through [insert information about what channels of communication will be monitored and factored into a student's final grade. For example, if the platform your school uses provides teachers with the chat logs of the general online classroom and private chats between particular students, it is important to note this information].

Your engagement will be assessed by [insert how engagement will be measured. This can range from the learning analytics tools employed to simple responses to questions in a classroom setting].

If you have concerns about any of these methods, please contact [teacher] for alternatives. We know that everyone's home learning environments look different, and we want to make sure that we're providing you with every opportunity to succeed during this time.

The shift to online learning due to the COVID-19 pandemic has spotlighted the prevalence of student data collection, use, sharing, and maintenance, and the need to adopt ethical and equitable practices to properly safeguard student privacy. Schools and districts are critical to the establishment of robust data governance programs and policies that protect student privacy. For those programs and policies to be most effective, schools and districts must also clearly and effectively communicate to their stakeholders—educators, parents, and students—the value of student data to better support students. Communicating that value and the associated policies and procedures to protect student data encourages prioritization of student privacy, better protection of student data, and the creation of a community-based culture of privacy.

We hope this toolkit provides a useful starting point as your school or district seeks to actively engage your school community to build trust and establish a culture of privacy in which each stakeholder is trained and motivated to protect student privacy in their particular role.

We encourage you to visit www.StudentPrivacyCompass.org for additional updates, resources, analyses, and professional development materials. You can also follow us on Twitter (@SPPrivacyCompass) for real-time updates on our work and reach out to us with questions at this link: <https://studentprivacycompass.org/contact-us/>.

Additional Resources

Student Privacy

- › [International Association of Privacy Professionals \(IAPP\): What is Privacy?](#)
- › [Data Quality Campaign \(DQC\): What is Student Data?](#)
- › [DQC: Who Uses Student Data?](#)
- › [Student Data Principles: 10 Foundational Principles for Using and Safeguarding Students' Personal Information](#)

- › [National Center for Education Statistics \(NCES\): Forum Guide to Education Data Privacy](#)
- › [DQC: Student Data Collection, Access and Storage: Separating Fact from Fiction](#)
- › [Virtru: Educate the Educators — A Lesson in Training Teachers and Staff to Protect K-12 Student Data](#)
- › [International Society for Technology in Education \(ISTE\): Standards for Students](#)
- › [Canadian Civil Liberties Association \(CCLA\): Peer Privacy Protector Project \(PPPP\)](#)

Data Governance

- › [US Department of Education Privacy Technical Assistance Center \(PTAC\): Data Governance and Stewardship](#)
- › [NCES: Forum Guide to Data Governance](#)
- › [Consortium for School Networking \(CoSN\): Trusted Learning From the Ground Up: Fundamental Data Governance Policies and Procedures](#)

Model Communications Tools

- › [Ventura County Office of Education, California](#)
- › [Denver Public Schools, Colorado](#)
- › [Cambridge Public Schools, Massachusetts](#)
- › [Raytown Quality Schools, Missouri](#)
- › [Utah Data Gateway Metadata Dictionary](#)
- › [Wisconsin Department of Public Instruction](#)
- › [Brandon-Evansville Public Schools: Responsible Technology Use Policy for Students](#)
- › [Denver Public Schools: Regulation of Use of Electronic Mail and Internet Systems](#)
- › [Louisiana Department of Education: Parental Consent Form for Universal Social, Emotional and Behavior Screener](#)
- › [ExcelinEd: Student Data Privacy Communications Toolkit](#)
- › [FPF: Effectively Communicating Student Data Privacy to Parents and Communities](#)
- › [New Zealand Government: Online Engagement](#)



ENDNOTES

- 1 Data Quality Campaign, What is Student Data?, (2015), Accessed November 24, 2020, <https://dataqualitycampaign.org/resource/what-is-student-data/>.
- 2 National Forum on Education Statistics, Forum Guide to Data Governance, (2020), Accessed on November 24, 2020, <https://nces.ed.gov/pubs2020/NFES2020083.pdf>.
- 3 CoSN Learning Education Innovation, Trusted Learning from the Ground Up: Fundamental Data Governance Policies and Procedures, (2019), Accessed November 24, 2020, <https://www.cosn.org/sites/default/files/TLE%20Data%20Governance%20Policies%20and%20Procedures%20Checklist.pdf>.
- 4 Trusted Learning Environment. (n.d.). Trusted Learning Environment Seal Program, Retrieved from <https://trustedlearning.org/>.
- 5 Student Data Principles. (n.d.). About the Principles, Retrieved at <https://studentdataprinciples.org/>.
- 6 Student Data Principles. (n.d.). 10 Foundational Principles for Using and Safeguarding Students' Personal Information, Retrieved from <http://studentdataprinciples.org/wp-content/uploads/2015/03/Student-Data-Principles-FINAL.pdf>.
- 7 Office of Educational Technology. (n.d.). Privacy, Retrieved at <https://tech.ed.gov/privacy/>.
- 8 Privacy Technical Assistance Center. (n.d.) Transparency Best Practices for Schools and Districts — Webinar Recording (2014), YouTube (March 10, 2017), Accessed November 24, 2020, https://www.youtube.com/watch?v=X9szbX1SK7Q&feature=youtu.be&ab_channel=PrivacyTechnicalAssistanceCenter.
- 9 North Dakota School Boards Association. (n.d.). Model: North Dakota Student Education Records Access and Amendment Procedure, Retrieved at <https://www.edutech.nodak.edu//sdp/files/2015/07/StudentRecordAccessAmendment.pdf>.
- 10 United States Department of Education. (Updated July 2015). Checklist for Developing School District Privacy Programs, Retrieved at <https://studentprivacy.ed.gov/resources/checklist-developing-school-district-privacy-programs>.
- 11 Trusted Learning Environment. (n.d.). Trusted Learning Environment Seal Program, Retrieved from <https://trustedlearning.org/>.
- 12 Kerry Gallagher, Larry Magid, and Kobie Pruitt, The Educators Guide to Student Data Privacy, (2016), Accessed November 24, 2020, https://studentprivacycompass.org/wp-content/uploads/2016/05/EduGuide_DataPrivacy_516.pdf.
- 13 Society for Technology in Education and Project Unicorn, A Practical Guide to Better Edtech Buying for Educators, (2020), Accessed November 24, 2020, <https://studentprivacycompass.org/resource/a-practical-guide-to-better-edtech-buying-for-educators/>.
- 14 Common Sense Privacy Program. (n.d.). Common Sense Policy Annotator Training — For Educators. Retrieved at <https://privacy.common-sense.org/resource/educator-privacy-training>.
- 15 Information and Privacy Commissioner of Ontario, New Lesson Plans for Educators: Privacy Rights, Digital Literacy and Online Safety, Information and Privacy Commissioner of Ontario Blog, (June 18, 2018), Accessed November 24, 2020, <https://www.ipc.on.ca/new-lesson-plans-for-educators-privacy-rights-digital-literacy-and-online-safety/>.
- 16 Student Privacy Compass, A Parents' Guide to Student Data Privacy, (2015), Accessed November 24, 2020, https://studentprivacycompass.org/wp-content/uploads/2015/09/parents_guide-1.pdf.
- 17 United States Department of Education. (n.d.). FERPA General Guidance for Parents. Retrieved at <https://www2.ed.gov/policy/gen/guid/fpco/ferpa/parents.html>.
- 18 Federal Trade Commission Consumer Information. (n.d.). Protecting Your Child's Privacy Online. Retrieved at <https://www.consumer.ftc.gov/articles/0031-protecting-your-childs-privacy-online>.
- 19 Nation Cybersecurity Alliance. (n.d.). Raising Digital Citizens. Retrieved at <https://staysafeonline.org/get-involved/at-home/raising-digital-citizens/>.
- 20 United States Department of Education. (n.d.) Protecting Student Privacy While Using Online Educational Services, YouTube (February 26, 2015), Accessed November 24, 2020, https://www.youtube.com/watch?v=deo2F19DK_o&feature=youtu.be&app=desktop&ab_channel=U.S.DepartmentofEducation.
- 21 CoSN Leading Education Innovation, Cybersecurity Considerations in a COVID-19 World, (2020), Accessed November 24, 2020, <https://www.cosn.org/sites/default/files/COVID-19%20%26%20Cybersecurity%20-%20Member%20Exclusive.pdf>.
- 22 International Society for Technology in Education. (n.d.). ISTE Standards for Students. Retrieved at <https://www.iste.org/standards/for-students>.
- 23 Surveillance Self-Defense. (Reviewed March 2, 2020). Privacy for Students. Retrieved at <https://ssd.eff.org/en/module/privacy-students>.
- 24 Canadian Civil Liberties Association. (n.d.). Peer Privacy Protector Project (PPPP). Retrieved at <https://ccla-pppp.squarespace.com/english-index>.
- 25 International Association of Privacy Professionals. (n.d.). What does Privacy Mean?. Retrieved at <https://iapp.org/about/what-is-privacy/>.
- 26 Data Quality Campaign, What is Student Data? (2016), Accessed November 24, 2020, <https://dataqualitycampaign.org/wp-content/uploads/2016/03/What-Is-Student-Data.pdf>.
- 27 Data Quality Campaign, Who Uses Student Data?, (2016), Accessed 24, 2020, <https://dataqualitycampaign.org/wp-content/uploads/2016/03/Who-Uses-Student-Data-Infographic.pdf>.
- 28 National Forum on Education Statistics, Forum Guide to Education Data Privacy, (2016), Accessed November 24, 2020, <https://nces.ed.gov/pubs2016/nfes2016096.pdf>.
- 29 Data Quality Campaign, Student Data Collection, Access, and Storage: Separating Fact from Fiction, (2016), Accessed November 24, 2020, <https://dataqualitycampaign.org/wp-content/uploads/2016/03/Student-Data-Collection-Fact-and-Fiction.pdf>.
- 30 Virtru Editorial Team, Educate the Educators — A Lesson in Training Teachers and Staff to Protect K-12 Student Data, Virtru Blog, (June 14, 2019), Accessed November 24, 2020, <https://www.virtu.com/blog/teachers-protect-student-data/>.
- 31 Data Quality Campaign. (n.d.) How Data Help Teachers, YouTube (January 15, 2014), accessed November 24, 2020, https://www.youtube.com/watch?v=cgrfiPvwDBw&feature=emb_title&app=desktop&ab_channel=DataQualityCampaign.

- 32 United States Department of Education Privacy Technical Assistance Center, Data Governance and Stewardship, (2015), Accessed November 24, 2020, https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Data_Governance_and_Stewardship_0.pdf.
- 33 National Forum on Education Statistics, Forum Guide to Data Governance, (2020), Accessed on November 24, 2020, <https://nces.ed.gov/pubs2020/NFES2020083.pdf>.
- 34 CoSN Learning Education Innovation, Trusted Learning from the Ground Up: Fundamental Data Governance Policies and Procedures, (2019), Accessed November 24, 2020, <https://www.cosn.org/sites/default/files/TLE%20Data%20Governance%20Policies%20and%20Procedures%20Checklist.pdf>.
- 35 Kelsey Finch, Nothing to Hide: Tools for Talking (and Listening) About Data Privacy for Integrated Data Systems, Future of Privacy Forum, (October 31, 2018), Accessed November 24, 2020, <https://fpf.org/2018/10/31/nothing-to-hide-tools-for-talking-and-listening-about-data-privacy-for-integrated-data-systems/#:~:text=In%20order%20to%20help%20IDS,the%20Nothing%20to%20Hide%20toolkit>.
- 36 Mark Schneiderman, Effectively Communicating Student Data Privacy to Parents and Communities, Student Privacy Compass, (June 14, 2017), Accessed November 24, 2020, <https://studentprivacycompass.org/schneiderman1/>.
- 37 New Zealand Government. (Updated October 20, 2020). Engagement. Retrieved at <https://www.digital.govt.nz/standards-and-guidance/engagement/>.
- 38 Ventura County Office of Education. (n.d.). Data Privacy, Safety and Security. Retrieved at <https://www.vcoe.org/Technology-Services/Data-Safety-and-Security>.
- 39 Denver Public Schools. (n.d.) Student Data Privacy. Retrieved at <https://academictechnologymenu.dpsk12.org/studentdataprivacy.aspx>.
- 40 Fairfax County Public Schools. (n.d.). Digital Privacy in FCPS. Retrieved at <https://www.fcps.edu/resources/technology/digital-citizenship-in-internet-safety/digital-privacy-fcps>.
- 41 Raytown Quality Schools. (n.d.). Technology. Retrieved at <https://www.raytownschools.org/site/Default.aspx?PageID=1541>.
- 42 Utah State Board of Education. (n.d.). Metadata Dictionary. Retrieved at <https://datagateway.schools.utah.gov/DataDictionary/Home>.
- 43 Wisconsin Department of Public Instruction. (n.d.). Student Data Privacy Main Menu. Retrieved at <https://dpi.wi.gov/wise/data-privacy>.
- 44 Student Data Principles. (n.d.). The Principles. Retrieved at <https://studentdataprinciples.org/the-principles/>.
- 45 Common Sense Privacy Program. (n.d.). Privacy Program. Retrieved at <https://privacy.commonsense.org/>.
- 46 Common Sense Privacy Program. (n.d.). Privacy Program. Retrieved at <https://privacy.commonsense.org/>.
- 47 PriBot. (n.d.). Home. Retrieved at <https://pribot.org/>.
- 48 Terms of Services; Didn't Read. (n.d.). Terms of Service; Didn't Read. Retrieved at <https://tosdr.org/>.
- 49 David Sallay and Amelia Vance, FAQs: The Protection of Pupil Rights Amendment, Student Privacy Compass, (March 27, 2020), Accessed November 24, 2020, <https://studentprivacycompass.org/faqs-ppra/>.
- 50 Common Sense Privacy Program. (n.d.). Privacy Program. Retrieved at <https://privacy.commonsense.org/>.
- 51 Student Data Principles. (n.d.). The Principles. Retrieved at <https://studentdataprinciples.org/the-principles/>.
- 52 Common Sense Privacy Program. (n.d.). Privacy Program. Retrieved at <https://privacy.commonsense.org/>.
- 53 Michele Molnar, Number of Ed-Tech Tools in Use Has Jumped 90 Percent Since School Closures, EdWeek Market Brief, (July 8, 2020), Accessed November 24, 2020, <https://marketbrief.edweek.org/marketplace-k-12/access-ed-tech-tools-jumped-90-percent-since-school-closures/>.
- 54 Learn Platform. (n.d.). Learn Platform. Retrieved at <https://learnplatform.com/>.
- 55 United States Department of Education Privacy Technical Assistance Center, Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices, (2014), Accessed November 24, 2020, https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Student%20Privacy%20and%20Online%20Educational%20Services%20%28February%202014%29_0.pdf.
- 56 Federal Trade Commission. (n.d.). Complying with COPPA: Frequently Asked Questions. Retrieved at <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0#N.%20COPPA%20AND%20SCHOOLS>.
- 57 Federal Trade Commission. (n.d.). Complying with COPPA: Frequently Asked Questions. Retrieved at <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0#N.%20COPPA%20AND%20SCHOOLS>.
- 58 Student Privacy Compass. (n.d.). Adopting EdTech: Privacy Vetting. Retrieved at <https://studentprivacycompass.org/resources/educator-training/#edtechvetting>.
- 59 United States Department of Education. (Updated March 2016). Protecting Student Privacy While Using Online Educational Services: Model Terms of Service. Retrieved at <https://studentprivacy.ed.gov/resources/protecting-student-privacy-while-using-online-educational-services-model-terms-service>.
- 60 Common Sense Privacy Program. (n.d.). Privacy Program. Retrieved at <https://privacy.commonsense.org/>.
- 61 CoSN Leading Education Innovation. (n.d.). Vetting Online Tools: Start with Privacy. Retrieved at <https://www.cosn.org/sites/default/files/CoSN%20Vetting%20Online%20Tools.pdf>.
- 62 Future of Privacy Forum. (n.d.). Student Privacy Pledge 2020. Retrieved at <https://studentprivacypledge.org/>.
- 63 Ventura County Office of Education. (n.d.). Student Data Privacy Check List. Retrieved at <https://www.vcoe.org/Technology-Services/Data-Privacy-Safety-and-Security/Teacher-Flowchart>.
- 64 Common Sense Privacy Program. (n.d.). All Common Sense Privacy Evaluations. Retrieved at <https://privacy.commonsense.org/evaluations/1>.

- 65 United States Department of Education. (March 30, 2020). FERPA and Virtual Learning during COVID-19 (Webinar Recording). Retrieved at <https://studentprivacy.ed.gov/training/ferpa-and-virtual-learning-during-covid-19-webinar-recording>.
- 66 United States Department of Education. (n.d.). FAQs on Photos and Videos under FERPA. Retrieved at <https://studentprivacy.ed.gov/faq/faqs-photos-and-videos-under-ferpa>.
- 67 CoSN Leading Education Innovation, Video Conferencing Tools in the Age of Remote Learning Privacy Considerations for New Technologies, (2004), Accessed November 24, 2020, <https://www.cosn.org/sites/default/files/Member%20Brief%20-%20Video%20Conferencing%20040120.pdf>.
- 68 Information Commissioner's Office. (n.p.). 4. Transparency. Retrieved at <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/4-transparency/>.
- 69 Information Commissioner's Office. (n.p.). Age Appropriate Design: a Code of Practice for Online Services. Retrieved at <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/>.
- 70 International Society for Technology in Education. (n.d.). ISTE Standards for Students. Retrieved at <https://www.iste.org/standards/for-students>.
- 71 Common Sense Education. (n.d.). Everything You Need to Teach Digital Citizenship. Retrieved at <https://www.commonsense.org/education/digital-citizenship>.
- 72 Canadian Civil Liberties Association. (n.d.). Peer Privacy Protector Project (PPPP). Retrieved at <https://ccla-pppp.squarespace.com/english-index>.
- 73 Google. (n.d.). Be Internet Awesome. Retrieved at https://beinternetawesome.withgoogle.com/en_us.
- 74 Montgomery County Public Schools. (n.d.). Responsible Use of Technology: Student Expectations. Retrieved at <https://www2.montgomery-schoolsmd.org/siteassets/schools/elementary-schools/t-w/travilahes/uploadedfiles/mediacenter/responsible-use-of-technology---student-expectations3.pdf>.

Education Data 101: A Briefing Book for Policymakers, Data Quality Campaign (December 2017), <https://dataqualitycampaign.org/wp-content/uploads/2017/12/DQC-EducationData101.pdf>.

Effectively Communicating Student Data Privacy to Parents and Communities, Future of Privacy Forum (June 14, 2017), <https://studentprivacycompass.org/schneiderman1/>.

FERPA & Virtual Learning During COVID-19, Student Privacy Policy Office, Privacy Technical Assistance Center, US Department of Education (March 30, 2020), https://studentprivacy.ed.gov/sites/default/files/resource_document/file/FERPAandVirtualLearning.pdf#a=.

Forum Guide to Data Governance, National Center for Education Statistics (June 2020), <https://nces.ed.gov/pubs2020/NFES2020083.pdf>.

Kelsey Finch, Nothing to Hide: Tools for Talking (and Listening) About Data Privacy for Integrated Data Systems, Future of Privacy Forum (October 2018), https://fpf.org/wp-content/uploads/2018/09/FPF-AISP_Nothing-to-Hide.pdf.

Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices, Privacy Technical Assistance Center, US Department of Education (February 2014), https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Student%20Privacy%20and%20Online%20Educational%20Services%20%28February%202014%29_0.pdf#a=.

Responsible Use of Technology: Student Expectations, Office of the Chief Technology Officer, Montgomery County Public Schools, <https://www2.montgomeryschoolsmd.org/siteassets/schools/elementary-schools/t-w/travilahes/uploadedfiles/mediacenter/fy20-studentcontractresponsible-use-of-technology2.pdf>.

Student Data Privacy Communications Toolkit, Excellence in Education (April 2016), <https://irp-cdn.multiscreensite.com/20c06e5c/files/uploaded/Student-Data-Privacy-Comms-Toolkit%5B11217%5D.pdf>.

Writing a Responsible Use Policy, Computer Explorers, <https://computerexplorers.com/Responsible-use-Policy-Template.pdf>.

