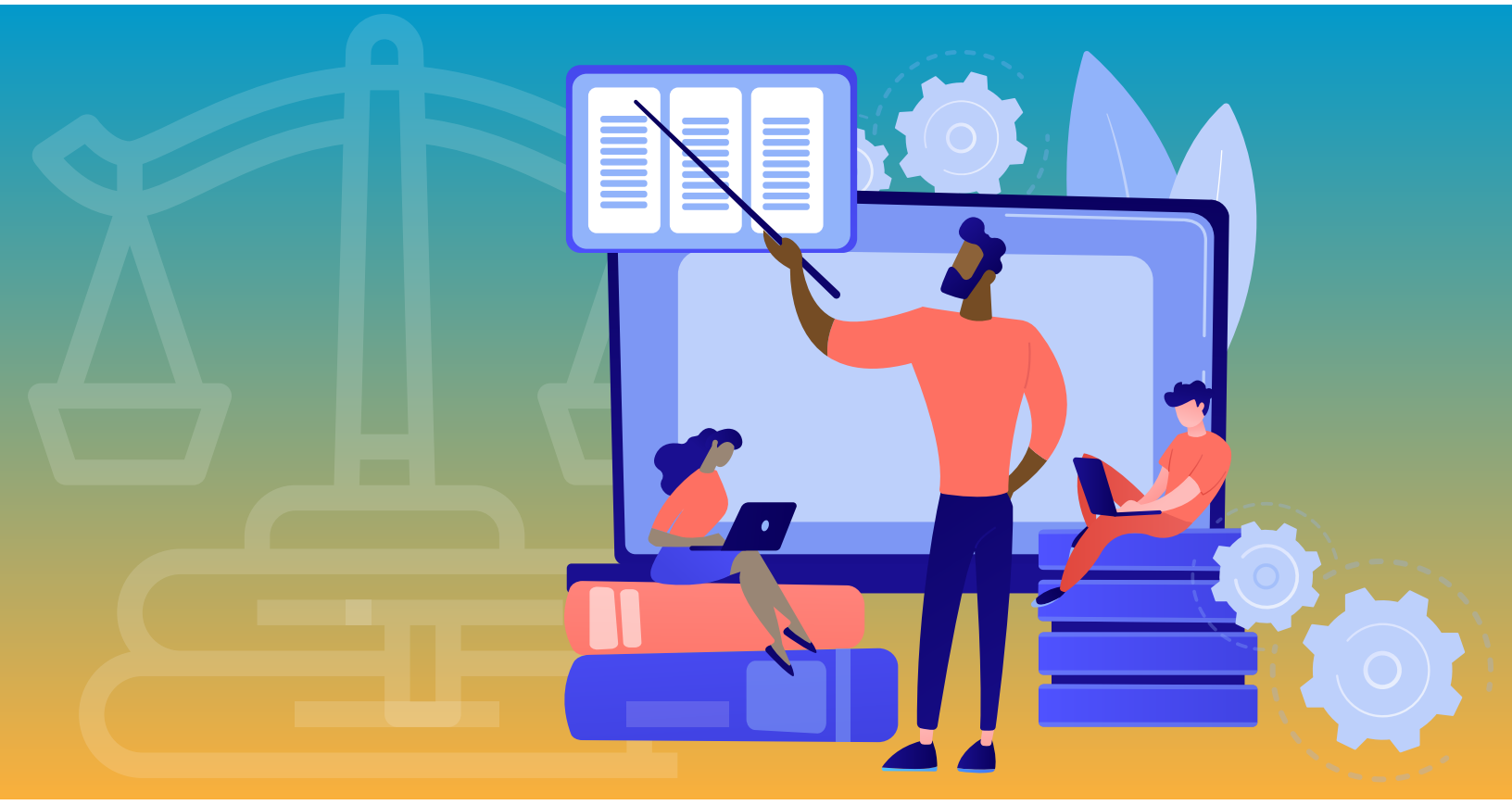
Student Privacy Best Practices Framework for State-Level Policies



FUTURE OF PRIVACY FORUM

TABLE OF CONTENTS

INTRODUCTION

Education agencies and institutions have always collected a wide range of data to allow teachers and school leaders to best serve every student. This data has traditionally included students' enrollment, academic, health, and disciplinary information. Education institutions now use digital technologies, such as resource libraries, learning management systems, and tools that allow students to collaborate with peers around the globe, which means they also collect and use students' personal data associated with these kinds of connected learning. As use of these technologies has vastly increased the amount of student data collected and shared, data privacy risks have also grown. These heightened risks mean that careful, effective student data privacy policies and practices are more important than ever to protect students, their data, and the learning opportunities that new technologies offer. While many states have passed student data privacy laws in the past decade, their effectiveness has been mixed, and few organizations have tracked the best practices and lessons learned from these laws. To help states create and maintain the best possible student data privacy policies and practices, Future of Privacy Forum (FPF) has created a Best Practices Framework for Student Data Privacy Policies (the framework).

This introduction briefly describes the value and risks of collecting and sharing student data, the context that has led to growing awareness of the need for better student data privacy, and FPF's framing of student data privacy in terms of responsibility, ethics, and equity. We then introduce the framework's six key elements.

Collecting and Sharing Student Data: Value and Risks

Effective collection and use of student data allows parents to track and promote their children's progress and helps teachers improve their instruction and more accurately meet students' needs. Student data also helps school and district leaders to make managerial decisions, allocate resources, and communicate with the public.[1] Constructive use of this data can increase the transparency and accountability of educational processes and help state and federal policymakers assess policies and strategies prior to the enactment of important changes.

Institutions collect this data throughout students' education journeys, and the data is shared not only within schools and districts but also potentially with other agencies at the state and local levels to improve student outcomes and services. For example, state longitudinal data systems (SLDS) may collect student data from early education programs through high school, college graduation, and career placement, to help states gain insights into health, economic, and education outcomes. This student data may also be combined with other state data sources (such as social services, financial services, and workforce data) to support student educational outcomes and employment opportunities.

While increased data collection and use can improve education by empowering students and teachers to enhance learning, it can also put sensitive student information at risk. A loss of autonomy, a stifling of creativity due to feeling surveilled, or even the public revelation of highly sensitive information such as financial data or disability status are a few of the many potential consequences of technology misuse, poor data security policies, or insufficient privacy controls. These risks require that all education stakeholders, agencies, and institutions develop and maintain strong student data privacy policies and practices.

Growing Awareness of Student Data Privacy

Education stakeholders have been concerned for decades about student privacy and responsible data use; the public has become increasingly aware of the vulnerability of digital data through high-profile consumer data breaches involving Yahoo,[2] Target,[3] and more recently, Equifax and LinkedIn.[4] Questions about data privacy have also arisen regarding education organizations, such as the nonprofit student-data management corporation InBloom, which shut down in 2014 as a result of stakeholders' mounting privacy concerns.[5] In the wake of the COVID-19 pandemic and associated massive shift to online learning, concerns about data privacy have intensified, given increased reliance on educational technology (edtech), heightened concerns

about students' privacy as they learn from their homes, and increased cybersecurity risks. Data gathered by LearnPlatform 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."

Even before the transition to online learning propelled by the pandemic, edtech tools had become indispensable to our K-12 education system. Schools and districts rely on hundreds[6] of third-party partners to enhance teaching and learning. Moreover, as noted above, K-12 school systems, higher education institutions, and SLDS are increasingly investing in the collection, use, and sharing of data to support improved student outcomes. This investment and expansion have also brought greater attention to student data privacy.

Effectively leveraging technology and student data requires that states address student data privacy issues. Attention to student privacy is necessary because students and parents are often not in the best position to assess the benefits and risks of data collection and use. They may lack time or expertise in privacy or security. How education agencies and institutions routinely use data can be difficult to understand and trust; schools have changed substantially since most adults were in the classroom. Student data privacy is also important because much student data collection, use, and sharing is involuntary: children are required to attend school, where they participate in activities that generate new data about them, such as completing online homework assignments. It is therefore vital that policymakers develop thoughtful approaches to student data privacy legislation, rules, policies, and technical safeguards that protect student data and can adapt to a quickly evolving technological environment.

Lawmakers' attempts to do this have yielded mixed results. Since 2013, policymakers have introduced nearly one-thousand student privacy bills in all 50 states, and 41 states and Washington, DC, have enacted more than 128 laws, whose scope and effectiveness vary by state.[7] Moreover, 21 states introduced 38 new proposals to protect student data in 2021.Unfortunately, state-level student data privacy laws have been fragmented and variable, creating robust student data privacy protections in some states and insufficient protections in others. Without clear, specific, and contextually appropriate legislative language, adequate training and resources to fund mandates, and proactive engagement with diverse stakeholders throughout the legislative process, student privacy laws may result in unintended consequences that can negatively impact student success and well-being. Effective policies enacted at the local, state, and federal levels can curtail the risks accompanying student data collection and ensure that data is used ethically to support learning.

Reframing Student Data Privacy: Responsible, Ethical, and Equitable Protections

These technological advances, privacy concerns, and legislative responses also invite deeper consideration of why attention to student data privacy is necessary and how stakeholders can best frame and enact it. Any data use creates both short- and long-term risks, and students are especially at risk because they lack the capacity to fully weigh the potential benefits and risks of data use. Privacy can support student success and give students agency over their own information and education. This means it is critical to ensure that education stakeholders use data not only effectively but also responsibly, ethically, and equitably in order to protect students' rights and well-being. Ethical student privacy protections require that data use aligns with established institutional values and societal norms. Equitable student privacy protections require that stakeholders use data to identify and address inequitable structures and systems of practice to improve outcomes for all students, especially those from historically marginalized groups.

Few organizations have tracked best practices and lessons learned from the immense shifts in the student privacy legal landscape over the past decade. This gap limits state policymakers' ability to pass and implement responsible, ethical, and equitable student data privacy policies and practices. To address this need, FPF has created a Best Practices Framework for Student Data Privacy Policies. The framework draws from data privacy scholarship and from exemplary student data privacy policies and practices to address student data privacy from diverse stakeholder perspectives and at multiple levels. These levels include

state and state institution/agency stakeholders involved in K-12 education, higher education, and SLDS. We also worked to weave data ethics and equity throughout the framework as a way to encourage responsible, student-centered use of data.

To holistically address student data privacy in multiple levels of the education system, we organize the framework according to the following six main objectives:

I. **State-level Commitment to Student Data Privacy.** Section one focuses on initial steps to create a foundation for protecting student privacy. This includes stating the purpose and applicability of state privacy policies, involving relevant stakeholders, designating student privacy leaders, and identifying institutional responsibilities. These initial steps allow the state to mitigate unintended consequences and begin to develop a culture of privacy throughout the state.

II. **State Student Data Privacy Policies**. Section two focuses on establishing policies to protect student data privacy. Establishing policies makes the state-level commitment to student privacy actionable. This includes providing clear definitions, establishing data use requirements, and including data sharing limitations.

III. **Education Agency and Institution Privacy Requirements**. Section three focuses on education agencies' and institutions' use and protection of data. To demonstrate ongoing commitment to safeguarding privacy, stakeholders should implement and evaluate over time written policies to protect both the security and privacy of data. This includes creating a written data governance plan, developing employee onboarding and offboarding protocols, and conducting ongoing assessments of the privacy impacts of data collected. These plans and protocols should comply with state student privacy policies.

IV. **A Statewide Transparency Plan.** Section four focuses on the need for all relevant parties in the data use process to proactively communicate and practice transparency regarding data use. This transparency plan should include clear communication, easily accessible public information, and opportunities for students and parents to provide input.

V. **Respect for Students and Their Data.** Section five addresses how to center students and their parents[8] in the data governance process. Empowering communities to get involved in the management of their data further promotes trust and accountability. This objective includes practicing fairness in data use; identifying and preventing bias and harm resulting from data use; using notice, choice, and consent mechanisms to promote engagement; practicing transparency and disclosure; and promoting data literacy.

VI. **Proactive Protection of Student Data Privacy.** Section six provides questions that can help preempt student data privacy issues before they arise. These questions relate to mitigating harm, addressing perception issues, and promoting accuracy and equity.

In the rest of this report, each of these sections outlines specific practices that support the main objectives, provides detailed justifications for the practices' inclusion in the framework, and includes checklists to help stakeholders ensure they have addressed each element. In this way, the framework helps state-level education stakeholders create responsible, ethical, and equitable student data privacy policies and practices. In addition, the framework provides much-needed guidance for establishing consistent legislation across states and for building a culture of privacy throughout state education agencies and institutions. The report concludes with a list of resources associated with the framework's development and with student data privacy in general.

Before we elaborate each objective's role in the framework, we clarify the definition of privacy in terms of student data; offer more detail on the privacy risks, harms, and hurdles related to student data; explain the student privacy legislative landscape, including more information on the need for responsible, ethical, and equitable student data policy; and outline our methodology for choosing the above-noted six objectives for protecting student data privacy.

DEFINING STUDENT DATA PRIVACY

Privacy is an amorphous concept, which people in different contexts define in various ways. One person may think of privacy as being alone in a private space, such as their bedroom. Another person may associate privacy with being free from surveillance, by their parents, their schools, or the government. Data privacy refers to information about individuals, but it still encompasses diverse concepts. Common conceptions of data privacy include the following:[9]

Data privacy as a *fundamental right*. Individual privacy rights are recognized in the US Constitution, the UN Declaration of Human Rights, and in over 80 countries around the world. Privacy rights also provide the foundation for other important rights, including self-determination and free expression.

- Data privacy's commonly understood aspects include a person's *control* over how their personal information "flows" between them and any third parties (how it is used and shared); a person's ability to explore without surveillance that hinders their freedom of thought or expression; a person's ability to protect their own dignity and reputation.
- Data privacy is *subjective*, as each person has unique privacy preferences and expectations. What feels invasive or creepy to one person may be innovative or cool to another. Many factors influence these preferences and expectations, including a person's familiarity with the entity or person collecting their data, whether a person is from a marginalized community whose data has been used in inequitable ways, their cultural background, and their trust in data-holding organizations.
- Data privacy is *contextual*. Whether it is appropriate to use or share personal data in a particular manner depends on ever-evolving social and ethical norms and on legal frameworks. To ensure that people understand an education agency's or institutional community's norms about integrating data, the agency or institution must communicate and engage directly with members of their community.

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

Since the introduction of these technologies and their unprecedented ability to collect and use data, stakeholders have talked about the word "privacy" as a form of fairness and power. The more information that one person or organization has about another, the more that party may influence or exert power over the other. Data privacy protections help individuals and communities maintain their autonomy and freedom when their governments and other organizations use their information.[10] For example, institutions, such as governments and companies, harvest and retain massive data sets on their citizens and users. This data is often collected from individuals without their knowledge or informed consent and can be used for purposes over which they have little to no control. In this context, data privacy helps to establish agreed-upon protections to affirm fairness, including the creation of transparent policies and practices that help correct power imbalances among the individual, the technology, and the institution.

Privacy, as a central component of fairness, often comes up in the educational context. **Student data privacy refers to the responsible, ethical, and equitable collection, use, sharing, and protection of student data.** Because students—especially younger children—are not fully equipped to weigh the potential benefits and risks of data collection and use, they require special privacy protections. They are also at risk for more-acute harms, such as opportunity loss, that may not fully emerge until later in life. Data privacy protections can support student success and give them agency over their own information and education.

Dispelling Misconceptions About Student Data Privacy

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

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

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

STUDENT DATA PRIVACY RISKS, HARMS, AND OBSTACLES

The widespread use of data-gathering technologies in consumer and education contexts has enabled numerous types of data privacy risks, such as unnecessary surveillance, careless storage practices, keeping individuals from knowing about or controlling their data, and bad actors who actively seek to steal or expose people's private information. This section outlines these risks and their potential harms to both students and education institutions and agencies, and it discusses some of the hurdles that institutions and agencies should consider in order to earn public trust regarding students' data.

Privacy scholar Daniel Solove has outlined types of general data privacy breaches and harms in terms of information collection, information processing, information dissemination, and invasion:[11]

A TAXONOMY OF PRIVACY BREACHES AND HARMS

Domain	Privacy Breach	Description
INFORMATION COLLECTION	Surveillance	Watching, listening to, or recording of an individual's activities
	Interrogation	Various forms of questioning or probing for information
INFORMATION PROCESSING	Aggregation	The combination of various pieces of data about a person
	Identification	Linking information to particular individuals
	Insecurity	Carelessness in protecting stored information from leaks and improper access
	Secondary Use	Use of information collected for one purpose for a different purpose without the data subject's consent
	Exclusion	Failure to allow the data subject to know about the data that others have about her and participate in its handling and use, including being barred from being able to access and correct errors
INFORMATION DISSEMINATION	Breach of Confidentiality	Breaking a promise to keep a person's information confidential
	Disclosure	Revelation of information about a person that impacts the way others judge her character
	Exposure	Revealing another's nudity, grief, or bodily functions
	Increased Accessibility	Amplifying the accessibility of information
	Blackmail	Threat to disclose personal information
	Appropriation	The use of the data subject's identity to serve the aims and interests of another
	Distortion	Dissemination of false or misleading information about individuals
INVASION	Intrusion	Invasive acts that disturb one's tranquillity or solitude
	Decisional Interference	Incursion into the data subject's decisions regarding her private affairs

Solove and privacy scholar Danielle Citron also created a useful typology of privacy harms:

TYPOLOGY OF PRIVACY HARMS	
Category	**Description**
PHYSICAL HARMS	Harms that result in bodily injury or death.
ECONOMIC HARMS	Harms that involve monetary losses or a loss in the value of something, such as a person's time or productivity, or an opportunity.
REPUTATIONAL HARMS	Harms that involve injuries to an individual's reputation and standing in the community–regardless of the accuracy of the information that caused that injury–that lead to a loss of esteem and/or result in lost business, employment, or social rejection.
PSYCHOLOGICAL HARMS	Harms that involve a range of negative mental responses, especially emotional distress–painful or unpleasant feelings--or disturbance–disruption to tranquility and peace of mind.
AUTONOMY HARMS	Harms that involve restricting, undermining, inhibiting, or unduly influencing people's choices. This can include (1) coercion — the impairment on people's freedom to act or choose; (2) manipulation — the undue influence over people's behavior or decision-making; (3) failure to inform — the failure to provide people with sufficient information to make decisions; (4) thwarted expectations — doing activities that undermine people's choices; (5) lack of control — the inability to make meaningful choices about one's data or prevent the potential future misuse of it; (6) chilling effects — inhibiting people from engaging in lawful activities.
DISCRIMINATION HARMS	Harms that involve entrenching inequality and disadvantaging people based on gender, race, national origin, sexual orientation, age, group membership, or other characteristics or affiliation. These harms thwart people's ability to have an equal chance to obtain and keep jobs, secure affordable insurance, find housing, and to pursue other crucial life opportunities, and cause broader negative societal effects.
RELATIONSHIP HARMS	Harms that involve causing damage to important relationships that are important for one's health, well-being, life activities, and functioning in society.

All of these risks and harms can manifest in ways specific to students and to education agencies and institutions, which we outline below.

Risks to Students

Often, concerns in the following areas, reflecting real or perceived data privacy risks, underpin student privacy controversies and dictate the content of student privacy laws, regulations, and policies:

RISK TO STUDENTS		
Risk	**Definition**	**How these concerns might be raised**
SAFETY	Personal or otherwise sensitive information may be revealed that could endanger students.	Is a stranger or someone dangerous able to communicate with my child or learn where my child lives?
OVER-COLLECTION & OVER-SURVEILLANCE	Over-collection and monitoring of student data and online activity can have chilling effects on students.	How much information is being collected about my child?
THE PERMANENT RECORD	Records of events, specifically mistakes, may be retained indefinitely, potentially leading to detailed profiles that negatively impact students' future opportunities.	Will my child's mistakes be recorded forever?
LOSS OF OPPORTUNITY	Student data can be used to make decisions about students and, specifically, can result in denials of opportunity.	What information will be used to make determine which opportunities my child doesn't have access to?
EQUITY CONCERNS	Students have varying access to devices or internet service, which has implications for safeguards in place and monitoring that occurs.	What if the information is biased? What if it is used in an inequitable way? What if my child and I can't or don't have access to the information or technology?
AGE-INAPPROPRIATE CONTENT	Students may access inappropriate websites and online content.	Is my child accessing content that isn't appropriate?
SOCIAL HARM	Revelation of personal and sensitive student information can result in stigmatization and cyberbullying.	Is my child being cyberbullied or stigmatized?
COMMERCIALIZATION	Companies may use student data to target students with advertisements and to build student profiles.	Are companies selling my child's data or targeting advertising to them?

Note that privacy risks may not always be immediately apparent. Many times, privacy risks for individuals are[12]

- **Incremental**: As data sets grow and are combined over time, so does the likelihood of a data breach, a reidentification attack (singling out individuals in seemingly nonpersonal data), or discriminatory impact on vulnerable, historically marginalized, and/or over-surveilled communities. For example, during the COVID-19 pandemic, K-12 administrators needed to communicate with their communities about COVID-19 infections while still protecting students' privacy. Specifically, schools needed to

ensure that when they informed their communities of infections, they did not directly or indirectly identify students.[13]

- **Unequal**: Privacy risks may also accrue unevenly throughout society. If stakeholders do not address these risks in advance, some community members may reap the benefits of data-driven governance while others bear the burden of privacy risks. For example, some schools require students to have their video cameras on during virtual classes. Video mandates raise privacy concerns for all students but particularly for students experiencing homelessness, an eviction, caretaker duties, and poor internet connectivity.[14]
- **Not Obvious**: Certain privacy risks are more impactful or more likely to occur for particular groups, and program designers who have not incorporated those groups' input may overlook those risks. For example, publishing the contact information of everyone who attended a meeting could be riskier for a family member who is a domestic violence survivor.
- **Intrusive**: Privacy is closely tied to feelings about self-control and autonomy, so the real or perceived loss of privacy can leave people feeling vulnerable, exposed, and out of control of their own lives. This loss can have a chilling effect on individuals' and communities' behavior, can harm relationships, and cause a loss of trust. For example, schools' increased reliance on surveillance technologies for school safety can result in hostile learning environments and can communicate to students that their schools have low expectations of them.[15]

Because privacy risks are numerous and varied, it is critical to engage diverse stakeholders in discussions and decision-making about data initiatives or technologies that rely on or will collect new student data.

Risks to Education Agencies and Institutions

Neither privacy risks nor public responses to them are hypothetical. When proper student data privacy protections are not in place and students suffer physical, emotional, or reputational harm due to unauthorized access to their personal information, education agencies and institutions face significant risks, some of which include the following:

- **Legal Consequences**: Education agencies and institutions may face fines, lawsuits, or even imprisonment for their failure to comply with federal and state student privacy laws.
- **Legislative Backlash**: Policymakers may impose new legislative restrictions on use and sharing of student data.
- **Withdrawal of Funding or Project Collapse**: Without proper student data privacy protections, technology or other promising learning initiatives may fail before they have a chance to succeed, leading to reduced funding or opportunity for other initiatives in the future.
- **Internal Protests**: School, district, and education agency and institution staff may object to policies that do not sufficiently protect student data, leading to lack of key support from teachers and administrators.
- **Public Relations Disaster and Lasting Mistrust**: Even if education agencies and institutions 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. Such a disaster can, in turn, lead to lasting mistrust among the public.

To reduce these risks, schools and districts are responsible not only for protecting student privacy but also for practicing transparency and building trust with school communities.

Obstacles to Earning Public Trust

As representatives of state and local governments, education agencies and institutions must be mindful that their use of individuals' personal data can be particularly fraught due to the following specific hurdles to earning public trust and social license to use personal data:[16]

- **Historical Misuse or Mistreatment of Data.** Both governments and researchers have mistreated or misused personal data. Education agencies and institutions should be aware that those scars linger, and appreciate that some individuals and communities have valid reasons to be reluctant to allow governments to share personal data.
- **Perceptions of Big Brother.** When government institutions collect and use data, privacy risks and people's fears can increase. To many communities, government agencies' frequent data collection, even for beneficial purposes, can feel indistinguishable from Big Brother-type surveillance. Historically marginalized populations, such as people of color and those living in poverty, may particularly be the target of multiple, concurrent data collection efforts by local, state, and federal agencies.
- **Companies' Misuse of Data and Data Breaches.** Numerous front-page headlines over the last decade have documented companies' misuse of data and data breaches, stoking fear and concerns about how much data companies collect and how they use and protect the data. This can erode trust in companies' handling of data and can lead people to believe that companies are concerned only about profit and their own self-interest. This erosion of trust causes issues in education given that many large companies, as part of their philanthropic endeavors, provide free or discounted edtech products to schools, but people who have taken to heart the phrase "if it is free, you are the product" often perceive these efforts with great skepticism.
- **Misconceptions of Consent.** Most privacy laws require organizations to obtain individuals' consent before using their personal information, particularly when the data is sensitive. The nature of the education system, however, means that consent is rarely obtained (and often is not feasible for education agencies or institutions to obtain). People may not realize the many ways in which schools, districts, education agencies, and institutions may legally use student data without the consent of students or parents, or people may simply expect an opportunity to consent by default.
- **Data-Driven Inequalities.** Conversations are growing among public, private, and academic education stakeholders about how data-driven tools may reflect or reinforce discrimination and bias, even inadvertently. Algorithmic systems' use of student data, through education agencies or institutions or their third-party vendors, raises serious ethical questions and may color public perceptions of other uses of student data.
- **Lack of Public Trust.** The perception that schools, districts, education agencies, and institutions will use personal data in unexpected ways or not keep the data private and secure can undermine individuals' and communities' trust in government. At its extreme, lack of trust means that individuals who are afraid of how data about them could be used may even provide false information or forgo government services.

Strong privacy protections and meaningful stakeholder engagement and communication can help to overcome these hurdles. Protecting privacy is critical to respecting individuals' rights and maintaining their trust in education agencies and institutions. If students and parents do not trust that their (or their children's) data will be protected or do not see the benefits of using student data for research, evidence-based policymaking, and supporting student success, they could characterize new data initiatives or technologies as tools of surveillance rather than as tools that will help students learn and begin successful careers.

STUDENT DATA PRIVACY LANDSCAPE: ANALYSIS AND CONTEXT

This section provides an overview of the rapidly evolving student data privacy landscape, to contextualize the laws, policies, and practices in the current student data privacy environment. It outlines the federal and state legislative environment in the US, describes the need for student data privacy laws to avoid unintended consequences, and develops the case for responsible, ethical, and equitable student data privacy policies and practice in order to meet the current needs of students and education institutions and agencies.

Current Student Privacy Legislative Landscape

The primary federal laws pertaining to student data privacy are the Family Educational Rights and Privacy Act of 1974 (FERPA), the Children's Online Privacy Protection Act (COPPA), and the Protection of Pupil Rights Amendment (PPRA).

Enacted in 1974, FERPA guarantees that parents have access to their children's education records and restricts who can access and use student information. Because FERPA's requirements are mandatory for education agencies and institutions that receive funding from the US Department of Education, the law applies in most K-12 schools and in many public and private post-secondary institutions. Regulators enforcing FERPA have the authority to investigate and require that schools remedy any violations, to prohibit schools from working with certain third parties, and to withhold all federal funds from education institutions that violate the law.

FERPA gives parents, guardians, or eligible students certain rights, including the right to inspect and review education records, the right to correct or delete inaccurate data, and the right to opt out of having a student's directory information published. FERPA generally protects student privacy by prohibiting schools from sharing education records with a third party without written consent from parents or eligible

students.[17] However, FERPA does permit schools to share information in a student's education record under certain circumstances without consent. For example, most edtech companies, such as gradebook systems or classroom learning management systems, receive student information under FERPA's "school official" exception. The exception allows schools to share education records with a third-party service provider if there is a "legitimate educational interest" in disclosing the information, the third party is performing a service the school would otherwise perform itself, and the third party is under the school's "direct control."

COPPA, which was enacted in 1998, requires operators of websites or online services that either have actual knowledge that a user is a child or that direct their services to children under age 13 to obtain verifiable parental consent before collecting personal information from children. While COPPA does not place any obligations directly on schools, COPPA allows schools to provide COPPA-required consent on behalf of parents when the operator uses information for an educational purpose and no other commercial purpose. If the operator uses information for a non-educational purpose, parents must be given the choice to consent (or not) to their children's use of that operator's service. The Federal Trade Commission (FTC) and state attorneys general enforce COPPA and have the power to investigate complaints, require violators to change their practices, levy fines, and enter into settlements.

PPRA gives parents, guardians, and students 18 or older certain rights when elementary or secondary schools administer surveys that include questions that fall under eight categories, such as political affiliation and religious practices of the student or parents.[18] Schools must obtain written consent before students participate in surveys that include questions from the eight categories. Additionally, schools must provide notice of surveys when information that could be used to identify a student is collected, shared, or used for marketing purposes. One important exception is that PPRA data restrictions do not apply to the collection, disclosure, or use of students' personal information for developing, evaluating, or providing educational products or services or to students or education institutions.

In addition to federal laws, state-level policymakers have enacted a wide variety of laws regarding student data collection and use by schools, companies, and state education agencies. They have done this in part to provide greater protection. For example, when schools, districts, and education agencies and institutions present choices about student data privacy to students and parents, the choices often reflect binary options that require either waiving privacy or opting out and taking potential learning opportunities away from children. Many state-level student privacy laws seek to address situations like these by providing special privacy protections to students. While states are responsible for protecting students' data and creating opportunities for students to engage with their data, the variability and complexity of the student data privacy legislative landscape are challenging for stakeholders who may not fully understand the protections and processes. These challenges can hinder effective implementation.

Since 2013, all 50 states and Washington, DC have proposed nearly one-thousand student privacy bills and have enacted more than 128 laws. Roughly half of US states have passed student privacy legislation modeled on California's Student Online Personal Information Protection Act (SOPIPA), which directly regulates edtech companies that provide services for K-12 students.[19] Other state laws regulate state or local education agencies. For example, Oklahoma's 2013 Student Data Accessibility, Transparency, and Accountability Act (Student DATA Act) establishes permissible state-level collection, security, access, and uses of student data.[20] These laws often include requirements for SLDS as well: Georgia's law S.B. 820, for example, includes rules about which data can be collected, how student data can be used, and who can access student data.[21]

While most state student privacy laws address K-12 settings, 22 percent of these laws also govern how public and private higher education institutions use student data. Unfortunately, many student privacy laws that apply to both K-12 and higher education settings do not effectively regulate higher education institutions, due to exceptions and ambiguity in the legislation. For example, a common provision exempts public higher education institutions from liability when they improperly disclose certain kinds of student

information, such as personally identifiable information, student records, and research records, when not otherwise allowable by another law.[22] In contrast, a more prescriptive Kentucky law mandates that public primary, secondary, and higher education institutions and their service providers create and implement data breach procedures,[23] and a Maryland law requires state public higher education institutions to enact privacy and security programs related to their systems.[24]

The Need for Responsible, Ethical, and Equitable Student Data Privacy Policy

Policymakers at both the state and federal levels have enacted proposals to protect student privacy, but even well-intentioned actions can create unintended consequences. Policymakers should be aware of past laws that have been reconsidered and revised in response to stakeholder feedback and unanticipated harms. For example, recent student privacy legislation in New Hampshire banned classroom recordings, resulting in barriers to completing teacher certification processes and students failing to receive accommodations prescribed in their Individualized Education Programs (IEP).[25] These unintended consequences forced legislators to clarify and update the legislation to reflect the intended purpose, which was ambiguous in the original law.[26] Yet, amending legislation takes time, and flawed legislation can harm the affected parties in the interim.

As outlined in the introduction, this framework conceptualizes student data privacy as the responsible, ethical, and equitable collection, use, sharing, and maintenance of student data.[27] Student data privacy policies and practices should therefore seek to ensure responsible, ethical, and equitable uses of data to minimize the risk of harm, especially to students from marginalized groups, such as students of color, students with disabilities, or students from lower socioeconomic backgrounds. Complying with existing laws and regulations alone may be insufficient to achieve these goals. Therefore, student data privacy conversations should start with establishing and seeking to practice basic assumptions of fairness.

Data ethics guide how stakeholders should govern, use, and protect data to minimize harm and risk. Examples of ethical data use include school districts setting up data governance policies and practices that establish which data can be collected, how long data can be used, who has access to data, and the purposes of data use. An ethical approach to data use includes policies that clearly delineate appropriate and inappropriate data practices and that communicate standards for protective use of data.

While data ethics focuses on ethical policies and practices, data equity focuses on using data to understand structural and systemic barriers to students' success and on taking actions to rectify those structures and systems. Equitable data practices include regular audits of data, data systems, and data practices to assess and remediate bias or discrimination. Examples of bias and discrimination include unequal surveillance and discipline of students of color and edtech use that does not comply with the Americans with Disabilities Act. Equitable data practices also include identifying and addressing achievement, resource, and opportunity gaps, such as unequal graduation rates, students' access to technology, and school district teacher shortages. A data equity mindset includes students (and their families) in the responsible and ethical use of their data. In practice, this includes regular communication to identify students' needs and realities and regularly informing students of their rights related to data collection and use.

FPF's best practices framework seeks to help stakeholders approach student privacy proactively and in ways that best serve students' needs, thereby working to circumvent reactionary policies and practices that may undermine educational opportunities for students. The framework can also help stakeholders develop best practices for the responsible, ethical, and equitable use of student data that helps schools achieve beneficial outcomes.

METHODOLOGY

This section outlines FPF's process of developing the best practices framework, specifying some key sources and how they informed our selection of the framework's six elements.

Framework Development

We developed this best practices framework through our expertise in data privacy scholarship, relevant laws, and current models of data privacy in both education and other types of other types of systems. These high-level resources are intended to serve a broad audience, ranging from state-level actors to students within the community. Through this evidence-based approach, the framework can establish best practices for policies seeking to protect education data privacy. The framework focuses on placing decisions about privacy and data in the hands of those who prioritize the protection and ethical treatment of the people whose data is collected. Moreover, students and parents should be empowered with the tools to understand and respond to how edtech companies and state education agencies and institutions handle their data.

The foundation of the framework was informed by two related proposals for model state student privacy laws. The Education Counsel's State Student Data Use, Privacy, and Security Legislation Checklist and the Foundation for Excellence in Education's Fundamental Student Data Privacy Principles served as illustrative guides for drafting specific elements in the framework. These two resources focus on educational data and establish the importance of individually delegating responsibilities around related policies and processes.

The Education Counsel's State Student Data Use, Privacy, and Security Legislation Checklist identifies the following items relating to state student privacy legislation:

- State the Purpose of the State's Privacy Law;
- Designate a State Leader for Protecting Education Data;
- Create a Data Inventory and Clearly Describe the Data Elements;
- Establish Policies to Promote Greater Public Transparency about Data Use;
- Identify Necessary Statewide Policies for Personally Identifiable Information;
- Require a Data Security Plan; and
- Apply Data Privacy and Security Policies to Contractors and Vendors.[28]

Similarly, the Foundation of Excellence in Education's (ExcelinEd) Fundamental Student Data Privacy Principles include the following elements:

- Value of Data;
- Openness;
- Limited Collection;
- Limited Use;
- Accurate and Accessible;
- Security; and
- Accountability.[29]

While their phrasing differs, these two resources reflect seven themes that are essential to effective and meaningful student privacy legislation:

1. **Clearly Explain the Benefits of Data Collection**
   It is vital that students and parents understand why a law allows the collection of educational data, and how such data collection stands to benefit students' learning. As such, state privacy legislation should clearly convey why a law allows schools and institutions to collect certain student data, as well as how such collection can be valuable to both students' academic success and a school's success in generating positive student outcomes. This theme embodies multiple principles from ExcelinEd and the Education Counsel's guidance, including the ExcelinEd openness principle and the Education Counsel's element about providing clear purposes for student privacy laws.

2. **Transparency**
   State laws governing student privacy should embody transparency. Schools and districts should clearly identify what student data they collect and explain their reasoning for collecting such data. Both the Education Counsel and ExcelinEd identify the importance of transparency in their principles, specifically in ExcelinEd's openness principle and the Education Counsel's public transparency element. Transparent communication about student data collection can help ensure that schools are thoughtful and conscious in their collection of student data. Moreover, such transparency stands to build trust among schools and districts with parents and students.

3. **Uniform Policies with Designated Leaders**
   While state privacy laws may vary, there are some universal components that should be present across a state's policies. This may mean a state appoints an authorized actor charged with directing and maintaining a state's student privacy systems. Uniform practices might also mean that there is a single policy that governs the process for parents to access their child's education records. Moreover, this theme requires that certain universal elements—like accuracy and availability for parent review—

be incorporated across a state's student privacy laws. This theme emulates Education Counsel's recommendation that legislation designate a state leader for protecting education data and identify statewide policies, as well as ExcelinEd's fundamental principle of accuracy and accessibility.

4. **Data Inventory Systems that Communicate Limited Use**
   The Education Counsel's Checklist encourages legislators to implement a data inventory that clearly lists the student data elements that a state collects and explains how the data is used. This theme also embodies the ExcelinEd fundamental principle of limited use, in that schools and districts must limit their use of student data to the purposes that the data inventory identifies.
5. **Establish Adequate Security Measures**
   Both the Education Counsel and ExcelinEd explicitly identify the importance of security measures in state student privacy laws. Secure data collection and storage are essential to responsible data governance, and help build trust in a state's data maintenance practices. Security measures include administrative, physical, and technical safeguards, and may involve annual audits and compliance evaluations.
6. **Due Diligence**
   This theme refers to Education Counsel's call for state legislation to implement certain privacy and security requirements with which vendors and contractors must comply, and ExcelinEd's fundamental principle of accountability. Ensuring that third party vendors and contractors, such as edtech companies, are bound by certain standards in their handling of student data holds third parties accountable. This theme requires that schools and districts exercise due diligence when entering into partnerships, and places data collection, maintenance, and security responsibilities onto third parties.
7. **Data Minimization**
   Finally, data minimization ensures that schools and districts limit the data they collect to information to which they have a legitimate educational interest. ExcelinEd calls for data minimization in its limited collection fundamental principle, and multiple of the Education Counsel's checklist items incorporate the idea that no more data than is necessary should be collected. Reporting requirements about what student data a school or district collects help ensure data minimization through conscious decision making by schools and educators about what kind of data collection is necessary for a student's success.

We then mapped these student privacy frameworks against two important sets of principles that underpin most privacy laws: the Fair Information Practice Principles (FIPPS) and the Privacy by Design principles (PbD). Developed in 1973 by an advisory committee of the US Department of Health, Education, and Welfare, the FIPPS are an ethical framework for protecting information and have influenced FERPA, the Privacy Act of 1974, and the European Union's General Data Protection Regulation.[30] The US Department of Homeland Security has since elucidated the FIPPS as follows:[31]

1. **Transparency:** Practice transparency and provide notice to individuals regarding collection, use, dissemination, and maintenance of personally identifiable information (PII).
2. **Individual Participation:** Involve individuals in the process of using PII, and to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII; provide mechanisms that allow individuals appropriate access, correction, and redress regarding their information.
3. **Purpose Specification:** Articulate the authority that permits the collection of PII and the purpose(s) for which the PII will be used.
4. **Data Minimization:** Collect only PII that is directly relevant and necessary to accomplish the specified purpose(s), and retain PII only for as long as is necessary to fulfill the specified purpose(s).
5. **Use Limitations:** Use PII solely for the purpose(s) specified in the notice; share with third parties only for a purpose compatible with the original purpose.
6. **Data and Integrity:** Ensure that PII is accurate, relevant, timely, and complete.

7. **Security:** Protect PII through appropriate safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
8. **Accountability and Auditing:** Establish accountability for complying with principles, provide training to all employees and contractors who use PII, and audit the actual use of PII, to demonstrate compliance with principles and all applicable privacy protection requirements.

The PbD principles, developed by Ann Cavoukian, Ph.D., while she was Information and Privacy Commissioner for the Canadian province of Ontario, foreground and center the data producer (for instance, a student). These principles can ensure more responsible, ethical, and equitable data uses. PbD does not seek to reduce the capabilities of data-driven organizations but, rather, demonstrates that it is possible to balance data privacy and data-driven success. Abiding by the principles mitigates the risks of student data privacy violations and harms while allowing state education systems to effectively and responsibly use data to better serve students. The PbD principles are as follows:

1. **Proactive not Reactive; Preventative not Remedial** means anticipating and preventing privacy risks before they occur.
2. **Privacy as the Default** means ensuring that systems and practices automatically protect personal data.
3. **Privacy Embedded into Design** means embedding privacy in the design and architecture of systems and practices so that privacy is an essential component of a product or service.
4. **Full Functionality––Positive-Sum, not Zero-Sum** means avoiding the false dichotomy of privacy versus security and seeking to accommodate all legitimate interests and objectives.
5. **End-to-End Security––Lifecycle Protection** means privacy is considered from the cradle to the grave, from collection to disposal of data.
6. **Visibility and Transparency** means assuring data producers and stakeholders that systems practices adhere to promises and objectives and that such adherence is subject to independent verification.
7. **Respect for User Privacy** means that individuals' best interests are the primary consideration.

Our goal in mapping the student privacy-specific recommendations to these broader models was to identify any major gaps in the student privacy frameworks that could help enhance our framework.

Then, we analyzed several additional privacy models and frameworks from education and other types of systems.

- Global Privacy Standard: Adopted at the 28th International Data Protection and Privacy Commissioners Conference in 2006, the Global Privacy Standard incorporates perspectives from the international data protection community. It informs technology developers and policymakers of concepts that may aid general data privacy protection, and these concepts impact the education space as well.
- Global Guidelines for Ethics in Learning Analytics: The Association for the Advancement of Computing in Education (AACE) developed these guidelines in response to the heightened use of predictive analytics in both K-12 and higher education systems. The report focuses on ethical decision-making, which prioritizes transparency and individual agency over data, among other ideas.
- Consumer Privacy Bill of Rights: Published by the Obama Administration in 2012, these principles go beyond educational purposes but are rooted in gaining consumers' trust and support through responsible management of their data privacy.

- National Institute of Standards and Technology (NIST) Privacy Framework: This framework focuses on managing privacy risk by prioritizing accountability and communication throughout an organization. It can apply to both education and non-education organizations, as data processing functions within an ecosystem of decision-makers.
- Information Systems Audit and Control Association (ISACA) Privacy Principles and Program Management Guide: Produced by ISACA, an international professional association focused on IT governance, this comprehensive framework provides 14 principles regarding educational privacy. The principles range from third-party/vendor management to security safeguards and accuracy and quality.
- Consortium for School Networking (CoSN) Trusted Learning From the Ground Up: Fundamental Data Governance Policies and Procedures: This resource provides an annotated checklist, which distinguishes policies and procedures, and identifies policy gaps in order to help organizations achieve a proper data governance system. This system includes how to use student data for research, training others on student data management, and establishing guidelines for data security.

We then supplemented the framework with additional knowledge that FPF has gained through our analysis of the hundreds of state student privacy laws introduced in all 50 states since 2014,[32] as well as the technical assistance FPF has provided to stakeholders in K-12, higher education, and SLDS over the past eight years. Considering interviews FPF has conducted over the past three years with 34 LEA and SEA staff representing 17 states, we also incorporated advice, lessons learned, and overall trends on how districts and states create cultures of privacy. Key elements that FPF has learned to look for when evaluating a state's student privacy landscape include the following:

- Whether state policies have enumerated responsibilities for each relevant party, including LEAs, the SEA (and, if separate, the SLDS agency), public and private higher education agencies and institutions, and vendors (especially education technology providers).
- Whether state policies incorporate aspects that mandate and/or facilitate the implementation of student privacy best practices, including
    - Adequate funding and resources (including staff or contractors with the relevant expertise with limited likely turnover);
    - Mandates that require written documentation and actions by staff, with sufficient penalties for lack of compliance, to incentivize prioritization of privacy;
    - Ongoing, substantive training requirements;
    - Ongoing, substantive transparency requirements;
    - Ongoing input and review by all relevant stakeholder groups (especially those working directly with students), given that implementation is more likely when stakeholders have been involved prior to passage of policies;
    - Feasible legal requirements; stakeholders will likely ignore impossibly high requirements in practice and will likely not follow low requirements, especially those lacking accountability in meeting those requirements. Low requirements can also provide a false sense of having sufficient privacy when, in fact, entities are still highly likely to be susceptible to legal, substantive, or perceived privacy risks.

Finally, it has become increasingly clear that, in order to prevent student data privacy crises (whether perception-based or substantive), policies must also include broad privacy guardrails that support good privacy practices as technologies and data practices evolve *and* as the types of data collected and data use change in schools. For example, many schools have the technological capability to track students' location when they use their personal or school devices to connect to campus internet, or to track every website students visit and every word they type on a school device or account (including when they access

an account on a personal device). Moreover, many education institutions are collecting new types of data regarding students' social-emotional growth or mental health, and other institutions are evolving beyond the traditional conception of schools to provide broader services, such as health care, to students.

Some of these new technologies, data collection, and data use may stretch the bounds of traditional social norms or represent a disconnect in that the education community assumes people expect something that students or parents actually find "creepy."[33] Some new data uses, particularly those furthest removed from the data's initial collection and purpose, may raise red flags for students and parents who do not understand why certain data should be shared beyond the education personnel directly serving them or their children. The ideal student privacy framework should incorporate privacy guardrails that protect current uses and that can proactively safeguard data privacy in future technologies, data collection, or data use. This is especially important because when privacy concerns are not adequately addressed, socially beneficial programs and initiatives will have limited impact or fail due to community pushback, lack of access to necessary data or limited adoption of new technologies, or the enactment of strict, fear-based privacy laws.

With the above considerations in mind, we identified a set of criteria for best practices, which should:

- Incorporate actionable student privacy practices that allow for valuable uses of data and technology in education to support students' success;
- Be crafted in consultation with state and local expertise;
- Be student-centered, by keeping student privacy needs and outcomes central to the creation of practical and actionable policies;
- Apply broadly but can be tailored to specific states' needs, processes, capacity, and interests;
- Reflect the best practices and lessons learned from student privacy laws introduced in the US since 2014;
- Be forward-looking and refer to newer and emerging technologies, to proactively address the future of student data privacy in teaching, learning, and educational data use.

Framework Components

As noted, we developed the framework to holistically address student data privacy as it exists in multiple levels of the education system. All recommended practices in the framework span state agencies and institutions that govern K-12, higher education, and SLDS. Because the state is foundational to establishing policies that support student data privacy best practices, the framework centers on governance by the state and state agencies and institutions.

I. **State-level Commitment to Student Data Privacy.** Section one focuses on initial steps to create a foundation for protecting student privacy. This includes stating the purpose and applicability of state privacy policies, involving relevant stakeholders, designating student privacy leaders, and identifying institutional responsibilities. These initial steps allow the state to mitigate unintended consequences and begin to develop a culture of privacy throughout the state.

II. **State Student Data Privacy Policies.** Section two focuses on establishing policies to protect student data privacy. Establishing policies makes the state-level commitment to student privacy actionable. This includes providing clear definitions, establishing data use requirements, and including data sharing limitations.

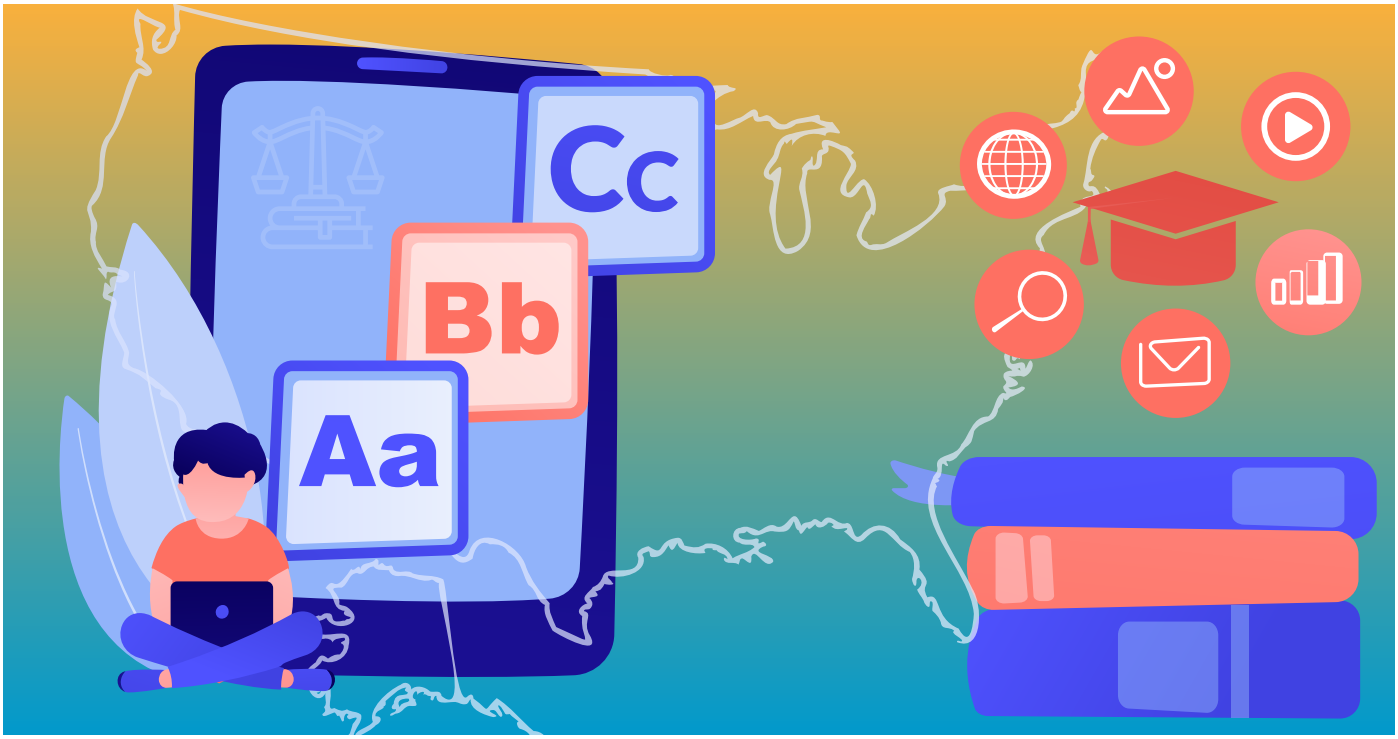
III. **Education Agency and Institution Privacy Requirements.** Section three focuses on education agencies and institutions' use and protection of data. To demonstrate ongoing commitment to

safeguarding privacy, stakeholders should implement and evaluate over time written policies to protect both the security and privacy of data. This includes creating a written data governance plan, developing employee onboarding and offboarding protocols, and conducting ongoing assessments of the privacy impacts of data collected. These plans and protocols should comply with state student privacy policies.

IV. **A Statewide Transparency Plan.** Section four focuses on the need for all relevant parties in the data use process to proactively communicate and practice transparency regarding data use. This transparency plan should include clear communication, easily accessible public information, and opportunities for students and parents to provide input.

V. **Respect for Students and Their Data.** Section five addresses how to center students and their parents[34] in the data governance process. Empowering communities to get involved in the management of their data further promotes trust and accountability. This objective includes practicing fairness in data use; identifying and preventing bias and harm resulting from data use; using notice, choice, and consent mechanisms to promote engagement; practicing transparency and disclosure; and promoting data literacy.

VI. **Proactive Protection of Student Data Privacy.** Section six provides questions that can help preempt student privacy issues before they arise. These questions relate to mitigating harm, addressing perception issues, and promoting accuracy and equity.



FRAMEWORK ELEMENTS

This section explains the best practices framework in detail. Organized according to the six objectives outlined above, this section describes each element of the framework objective and justifies the element's importance for a state seeking to be a model of student data privacy. Many of the descriptions include examples of the element in practice and how states seeking to be student data privacy exemplars can achieve the element.

The Framework

I. STATE-LEVEL COMMITMENT TO STUDENT DATA PRIVACY

A state's commitment to student data privacy is the first step in ensuring that the state has set up basic elements needed to protect student privacy. Making a state-level commitment requires stating the purpose and applicability of state data privacy policies, involving relevant stakeholders in the policy development process, designating leaders in student privacy and data governance, and identifying institutional responsibilities for student privacy.

Student data privacy laws and policies can often have unintended consequences that governing bodies do not anticipate. Stating a privacy law's purpose and applicability explains the problem the law seeks to solve and identifies responsible parties. Additionally, articulating the purpose and applicability can acknowledge the competing interests associated with solving student data privacy problems. While student privacy is valuable, a perceived competing value is that the use of student data can result in beneficial outcomes for students and other stakeholders. Stating the purpose and applicability of state privacy policies shows stakeholders that policymakers have carefully considered these concerns and that the state has committed to protect students' data privacy.

Involving relevant stakeholders in the policy development process can also mitigate unintended consequences. Policymakers may not always fully understand how a policy may play out in practice or how

to best tailor a policy to achieve the intended purpose and applicability. Involving relevant stakeholders ensures that multiple perspectives inform the development process, and provides a voice to those who may either implement or be affected by the policies.

Designating leaders in student privacy and data governance also strengthens the state-level commitment to student privacy. Designated leaders act as a bridge between state policy and local practice. Designated leaders can be a point of contact so that interested parties know where to find information, demonstrate the state's commitment to student data privacy, and foster trust in the state's data governance policies and processes. Additionally, they can work to ensure accountability throughout the state, overseeing and regularly reviewing implementation of privacy and data-related goals. Similarly, identifying institutional responsibilities for student privacy and data governance clearly communicates the agency's or institution's role in the state's student privacy commitments.

Stating the purpose of policies, involving relevant stakeholders, designating leaders, and identifying institutional responsibilities create a state-level commitment that acts as a foundation on which the state can build as it works toward becoming an exemplar of student data privacy. These are the first steps needed to build a culture of privacy throughout the state and to ensure the successful implementation of data governance plans.

STATE-LEVEL COMMITMENT TO STUDENT DATA PRIVACY
IA. State the Purpose and Applicability of State Privacy Policies
1) Each policy states its purpose or intent.
2) Each policy clearly states which entities are covered by that policy, such as the state and local education agencies, public and private institutions of higher education, vendors, and statewide longitudinal data systems (SLDS).
3) A state policy or policies govern student privacy requirements for state education agencies, including state longitudinal data systems, local education agencies, public and private institutions of higher education, and third parties.

1) Each policy states its purpose or intent.

The purpose, or intent, of the policy should be stated in order to promote transparency and gain support from relevant stakeholders. The purpose or intent will guide the state and state actors in carrying out the objectives outlined in the policy. As noted, student data privacy laws can often have unintended consequences, so stating the law's purpose serves to remind the courts and communities that the legislature thoughtfully addressed student privacy concerns, and this articulated statement will provide clarity and transparency if any unintended consequences arise. For example, Nebraska's student data privacy law achieves this best practice by including the stated purpose in the policy: "The Legislature finds and declares that the sharing of student data, records, and information among school districts, educational service units, learning communities, and the State Department of Education, to the fullest extent practicable and permitted by law, is vital to advancing education in this state."[35]

In order to avoid unintended consequences, policy should avoid being overly broad and, instead, should prohibit only activities that would cause harm to individuals. Louisiana policymakers enacted an overly broad policy with harsh penalties in 2015.[36] The law stated that teachers could receive jail time for sharing any data nonconsensually, even if it was an accident. The fear of fines and imprisonment prevented Louisiana schools from submitting students' names to the state scholarship fund, which harmed vulnerable students from families that needed the scholarships.[37]

While a broad purpose statement can be better than no purpose statement, vague statements that identify general concern can lead to a misidentification of the problem or need that the policy seeks to address.

Such confusion can lead to erroneous or inconsistent implementation of the policy.To assess implementation of this element, education agencies and institutions must ask whether the law clearly states its purpose and whether there is a process for feedback and rectification if unintended consequences arise during the policy's implementation.

2) Each policy clearly states which entities the policy covers, such as state and local education agencies, public and private institutions of higher education, vendors, and statewide longitudinal data systems (SLDS).

Effective student privacy legislation identifies the entities responsible for carrying out individual policies. Clear delegation of responsibilities helps prevent inappropriate shifting of responsibilities to parties unequipped to carry out policies. The purpose, requirements, and enforcement will also likely differ based on the covered entity. Therefore, stating the covered entity should be a primary consideration to properly frame the policy. For example, in their agreements, some third-party vendors shifted their COPPA responsibilities for obtaining verifiable parental consent to schools, even though companies, not education institutions, are subject to and responsible for complying with the law. Lack of clarity on the responsible party resulted in confusion, diffusion of responsibility, and evasion.

3) A state policy or policies govern student privacy requirements for state education agencies, including state longitudinal data systems, local education agencies, public and private institutions of higher education, and third parties.

State policymakers should ensure that there are policies protecting student privacy that include responsibilities for all appropriate parties, including state and local education agencies, public and private institutions of higher education, Edtech companies, and SLDSs. This comprehensiveness is necessary to hold accountable entities with access to student information, and to ensure all relevant parties collectively share the responsibility of and have a vested interest in protecting student privacy. Each enumerated party is a student privacy stakeholder and should be expressly responsible for prioritizing student privacy. By sharing this responsibility, stakeholders have an interest in ensuring that both their own practices and those of their counterparts align with the state's requirements. To assess the implementation of this element, educational agencies and institutions must ask whether the state has separate binding policies—be it a law, regulation, or other policy—and whether these policies govern the practices of the SEAs, LEAs, public and private institutes of higher education, vendors, and SLDSs, respectively. California has an Education Data Governance program that helps educators and school districts standardize their governance practices across the state by providing support for data-related policy, procedure and role development.[38]

IB. Ensure Relevant Stakeholders Are Included in Developing Policy and Evaluating Implementation

1) The policymaking process ensures that all major stakeholders likely to be impacted by a policy have an opportunity to provide feedback and discuss potential unintended consequences of any part of the policy.

2) The policy establishes a mechanism to revisit the policy's effects after sufficient time for implementation, including an opportunity for stakeholders to give feedback.

1) The policymaking process ensures that all major stakeholders likely to be impacted by a policy have an opportunity to provide feedback and discuss potential unintended consequences of any part of the policy.

The state should engage all stakeholders likely to be impacted by the policy in order to prevent unintended consequences. Any student data privacy policy is likely to impact students, teachers, parents, tech companies, school administrators, and state leaders. These parties, especially at the district level, will be responsible for implementing policies and thus are best equipped to identify and develop methods for mitigating incidental negative impacts. For example, several states sought to prohibit districts from carrying student data on "portable media devices." This ban would have entirely prevented schools' and districts' use of cameras.[39] A similar situation occurred in 2015, when New Hampshire prevented teachers from recording classes without the school board's written permission, which prevented students with disabilities from receiving remote instruction necessitated by their IEPs.[40] Had policymakers consulted special education instructors or students with disabilities and their advocates during the drafting process, these unintended consequences would likely not have occurred and students would not have been harmed.

Stakeholder engagement should include meaningful communications with people who will implement these policies and with people whom these policies will likely affect. At an early stage, policymakers should take the time to identify potential stakeholders and consider their interests and positions.[41]

A potential model for collecting feedback involves convening a student data privacy council composed of representatives from diverse stakeholder groups. West Virginia has held public, statewide forums to inform the community on student data privacy efforts.[42] In 2016, Utah passed a law requiring the establishment of a "data users advisory group" made up of individuals who regularly use student data in schools and districts. According to the bill, the advisory group would be tasked with providing feedback about the feasibility of proposed student privacy laws and regulations.[43] Involving stakeholders with diverse perspectives and experiences ensures that the policies are comprehensive, equitable, and relevant to practices.

2) The policy establishes a mechanism to revisit the policy's effects after sufficient time for implementation, including an opportunity for stakeholders to give feedback.

Well-intentioned state laws governing student data can have unintended consequences on student privacy. These unintended consequences can result in harm to students or disruption of their educational experience, so it is vital that remedial policies exist and problems are addressed immediately. In 2013, an Oklahoma rule that required redacting data that listed fewer than 10 students prevented 58 percent of districts from reporting their graduation rates. In smaller districts with very high or very low graduation percentages, some had fewer than 10 students who graduated or failed to graduate. This meant that these districts were prohibited from publishing their unredacted graduation percentages.[44] Under Oklahoma law, the earliest the Oklahoma state legislature could have addressed this problem was 2016. However, because the law included a countermand clause, the Oklahoma State Board of Education was able to revoke the rule sooner.[45]

The Connecticut state legislature also underwent multiple amendments of their student privacy law, originally passed in 2016 and then amended in both 2017 and 2018.[46] Stakeholders believed the original law required a contract between school districts and anyone with whom the district shared student data. In practice, this resulted in hundreds of individually negotiated contracts because even if only two students in a district used a particular software for an IEP, the district had to complete a contract with the vendor, binding it to the Connecticut privacy law. The 2017 amendment moved the law's effective date to 2018 to give districts and vendors more time to comply. At a hearing in 2017, Executive Director of the Connecticut Association of Public School Superintendents said, "I also don't think that any of us fully understood the implications of the Act once it got down to it, especially to the classroom level."[47] Considering this stakeholder feedback and implementation challenges, policymakers amended the law again in 2018 to address consequences the 2017 amendment had not fully resolved. For example, the amendment established a central database that allowed educators to identify companies that had signed Connecticut's Student Data Privacy Pledge

and agreed to comply with the Connecticut law. Although Connecticut underwent multiple rounds of amendments, the original law established a task force to study issues relating to student data privacy and make recommendations to improve the state's privacy policies. By creating this task force, Connecticut ensured that its policies could be implemented and that stakeholders could provide recommendations to improve the process.

Additionally, Maryland engaged stakeholders through its Student Data Privacy Council, established in 2019 by the state's legislature to evaluate the state's Student Privacy Act of 2015. The Council has a diverse makeup of stakeholders so as to include teacher, parent, legal, academic, administrative, and industry perspectives. In addition to evaluating and making recommendations regarding the state's 2015 law, the Council is also tasked with reviewing similar laws, studying evolving technology and best practices relating to student privacy, and evaluating the state's ongoing student privacy practices.[48] Councils like Maryland's Student Data Privacy Council are incredibly valuable in developing effective student privacy policies and evaluating legislation from a variety of angles.

Moreover, as the privacy landscape continues to evolve, policies that govern student privacy may need amendments after implementation. For these reasons, policies should include built-in mechanisms that allow the legislature to efficiently implement necessary changes and ultimately enhance effectiveness.

IC. Designate Student Privacy and Data Governance Leaders

1) Policies designate at least one responsible party (either a person or a group) in charge of student data privacy and data governance within each relevant education agency and institution.

2) Policies clarify the scope of each responsible party's role and responsibilities.

3) Policies identify each responsible party's qualifications or compositional requirements.

4) Policies establish necessary ongoing funding and resources to support each responsible party's role and work.

5) Policies detail the responsibilities and authority of the student privacy and data governance leaders at the state and local levels.

6) Policies grant rulemaking authority to student data privacy leaders or specified policymakers.

1) Policies designate at least one responsible party (either a person or a group) in charge of student data privacy and data governance within each relevant education agency and institution.

Within each education agency and institution, at least one responsible party should be responsible for overseeing and supporting student data privacy and data governance efforts. Designating specific privacy leaders helps an agency or institution promote visibility and accountability for adherence to the state's privacy policies. Moreover, such appointments work to develop a privacy-centric culture within the educational agency or institution. Several state student privacy laws, including in Utah,[49] New York,[50] Virginia,[51] and West Virginia,[52] require the appointment of a chief privacy officer at the state education agency. Mandated appointment of privacy leaders signals the importance of student privacy and responsible data practices for each agency and institution and assures that education agencies and institutions have a resource for guidance.[53] These leaders do not need to be individually appointed officers. Policies may establish an education data oversight and governance board tasked with ensuring that responsible state actors at each participating state agency and institution assist, collaborate, and ensure consistency in data privacy and security practices. This may be

especially useful in smaller districts that do not have the capacity to hire a chief privacy officer; rather, they might have a group that meets regularly to discuss privacy strategy.[54]

However, the Institute of Education Sciences warns that bringing in too many voices can hinder the development of effective policies and practices.[55] Policies should therefore strive to balance between ensuring that all important voices are at the table and having a group small enough to be successful.

2) Policies clarify the scope of each responsible party's role and responsibilities.

When identifying responsible parties for student privacy and data governance, policies should ensure that each role has distinct, clearly outlined responsibilities. This will ensure proper allocation of funding and that specific actors cover all aspects of student privacy and data governance. Furthermore, this prevents responsible parties from overlapping student privacy and/or data governance commitments.

When identifying these roles and responsibilities, policies should task responsible privacy leaders with developing standards and processes for providing information to students, parents, and the public on proposed significant data initiatives, including their purpose(s) and how data will be used; opportunities for students, parents/legal guardians, and the public to raise questions, concerns, and issues regarding such initiatives; and data privacy and security protections. Additionally, outlining the scope of the state privacy leaders' authority provides clarity to other parties who bear responsibilities within the policy. This alleviates ambiguity and confusion regarding each party's responsibility. For example, Utah's law specifies the chief privacy officer's responsibilities, which include ensuring compliance with student privacy laws, investigating complaints of alleged violations of the law, and reporting violations.[56] New York's student privacy law also created the role of a chief privacy officer, who is tasked with investigating complaints of third-party noncompliance with the state's student privacy law and regulations.[57] In addition to chief privacy officers, other student privacy leadership positions should also have a clearly defined scope of responsibilities. The Kansas Department of Education has created policies, outlined in the data governance program handbook that define the role and scope of responsibility of the data governance board in establishing and enforcing policies related to agency data management, and the role of data owners and data stewards.

3) Policies identify each responsible party's qualifications or compositional requirements.

The state must also identify the required qualifications for individuals or the compositional requirements for a governing body. For example, in New York, the state requires a chief privacy officer who is "qualified by training or experience in state and federal education privacy laws and regulations, civil liberties, information technology, and information security."[58] Additionally, the members of the federal Commission on Evidence-Based Policymaking were required to have expertise "in protecting personally identifiable information and data minimization."[59] Requiring certain technical expertise or background knowledge ensures that responsible parties tasked with developing and maintaining student privacy and data governance programs have the tools to succeed.

4) Policies establish necessary ongoing funding and resources to support each responsible party's role and work.

Without proper funding and resources, responsible parties cannot comply with the policy. By requiring a monetary commitment to student data privacy at the state level, the policy prioritizes the advancement of student data privacy and data governance efforts. Funding helps ensure that responsible parties can build teams with technical expertise, develop resources and guidance, and ensure compliance with relevant policies. Utah dedicated funding not only to the state board of education's chief privacy officer role but also to student data privacy auditor and student data privacy project manager positions to support the chief privacy officer's work, thereby greatly augmenting the state's student privacy capabilities.[60] West Virginia similarly requires that the state superintendent appoint a Data Governance Manager that is responsible for safeguarding student data privacy; specifically, ensuring adopted technology and SLDS data are compliant with privacy and security policies and maintaining engagement with the public, amongst other

responsibilities.[61]Funding should be provided continually as needed rather than in a one-time allocation, to demonstrate long-term prioritization of student data privacy and to acknowledge its evolving nature. Schools are more vulnerable to data breaches and ransomware attacks when they do not fund student privacy and data security, which may therefore end up being far more costly. In some instances, this has caused not only a loss of data but also traumatic experiences for communities that endure explicit threats from hackers demanding their data.[62]

5) Policies detail the responsibilities and authority of the student privacy and data governance leaders at the state and local levels.

It is essential that student privacy and data governance leaders are appointed at both the state and local levels. If leaders responsible for student privacy and data governance exist only at either the state or local level, rather than both, the statewide approach to student privacy and data governance will be imbalanced and will likely fail at scale. For example, Florida regulation places the responsibility to maintain the privacy of student records on school district principals; any data that falls outside of the principal's purview would be the responsibility of the superintendent of schools.[63] In Alaska, each district is required to assign one employee the duty to protect the confidentiality of student personally identifiable information.[64] Balancing student privacy responsibilities at different levels ensures that appropriate resources are context-specific and disseminated throughout the education system. Furthermore, ensuring that designated stakeholders prioritize student privacy and data governance at multiple levels creates a sense of accountability and fosters a culture of privacy throughout the state's education ecosystem. Privacy and data governance programs grow stronger when there are multi-level stakeholders that define context-specific, practical, and relevant privacy practices for education agencies and institutions. Additionally, this allows education agencies and institutions to prioritize diversity and innovation in their student data governance models and to account for unique local circumstances.

6) Policies grant rulemaking authority to student data privacy leaders or specified policymakers.

Building a culture of privacy is an evolving process whereby the entire community is involved in creating an environment that protects student data privacy.[65] Therefore, policies may need to similarly evolve as education agencies and institutions refine their privacy practices. Since needs may arise for new policies not considered or outlined in the original legislation, state agencies and local privacy leaders should have some authority to update policies to reflect the current privacy landscape. Empowering privacy leaders to make changes and introduce new rules into state policies ensures that a state's privacy practices are always improving, rather than remaining stagnant.

Technology rapidly changes, and new, valuable uses of student data emerge. Privacy guardrails are needed for these new uses and technologies, to preserve trust between students and education agencies and institutions. However, most state legislatures only meet for a few months each year, and legislators rarely have a deep understanding of how schools operate. Consequently, it is important that privacy leaders with expertise and understanding of the implications of student data collection have the authority to make timely, relevant changes. This is nothing new for some states. For nearly a decade, New Jersey's State Board of Education (SBE) has had the authority to "provide by regulation for the creation, maintenance, and retention of" student records.[66] This New Jersey statute grants its SBE broader authority related to student records in general. Similar rulemaking authority exists within Idaho legislation relating to the safeguarding of student data.[67] Similarly, New York directs the Commissioner of Education, in partnership with the Department of Education's Chief Privacy Officer, to set standards for educational agency data security and privacy policies.[68] A more recent trend has states granting their SBEs authority relating specifically to student data privacy. For instance, West Virginia and Nebraska have empowered their SBEs to engage in student privacy policymaking by providing guidance and writing rules.[69] Some states have extended SBEs' authority further by allowing them to supersede or countermand policies within state legislation.[70]

Additionally, as stakeholders continue to build and evolve the state's data governance plans, the need to monitor and investigate compliance with policies will increase. State agencies should have the flexibility

to improve their compliance process over time. It is also helpful to specify whether a student privacy governing body or other state policymakers have policymaking authority, whether in the form of binding policies or simply offering guidance. For example, Oklahoma's Student Data Accessibility, Transparency and Accountability Act of 2013 required the SBE to adopt rules implementing the act's provisions, such as creating, publishing, and making publicly available an inventory of student data and creating a data security plan.[71] Allocating authority to SBEs not only benefits legislatures by ensuring that state policies reflect schools' evolving needs, but it also strengthens the roles of SBEs.[72]

> "any new student data collection proposed by the State Board of Education becomes a provisional requirement to allow districts and their local data system vendors the opportunity to meet the new requirement . . ." 70 OK Stat. § 70-3-168 (I)(C)(7)(a)(1) (2014).

ID. Identify Institutional Responsibilities for Student Privacy and Data Governance

1) Policies clearly state responsibilities related to data governance and privacy measures for the state education agency (and, if separate, the SLDS), local education agencies, and higher education institutions.

2) Policies clearly distinguish the student privacy and data governance responsibilities and authority for the state education agency (and, if separate, the SLDS), local education agencies, and higher education institutions.

3) Policies require a written data governance plan and processes.

1) Policies clearly state responsibilities related to data governance and privacy measures for the state education agency (and, if separate, the SLDS), local education agencies, and higher education institutions.

Due to the many options and challenges in developing data governance and privacy protections, the state should specify the responsibilities of each designated education agency and institution in order to ensure that all entities establish strong programs. Each agency and institution plays a separate, context-specific role in safeguarding student data, and to ensure efficiency and effectiveness it is vital that these roles are clear. Individuals and entities tasked with developing, enforcing, maintaining, or otherwise handling student data must know exactly which tasks they are responsible for and which tasks have been delegated elsewhere.

Beyond assigning specific responsibilities to entities, policies should also clarify which tasks are required and which tasks are absolutely necessary. This allows state and local entities to prioritize their responsibilities and properly allocate resources. A clearly articulated data governance plan and processes are invaluable to ensuring transparency and accountability; clearly defining roles; minimizing inefficiencies such as duplicated efforts or continuation of outdated practices; maintaining accurate, complete, and fair data; preventing data misinterpretations or misrepresentations; and promoting a culture of privacy.[73]

2) Policies clearly distinguish the student privacy and data governance responsibilities and authority for the state education agency (and, if separate, the SLDS), local education agencies, and higher education institutions.

State education agencies, local education agencies, and higher education institutions each have unique student privacy and data governance responsibilities due to varying institutional processes and functions. Therefore, each should serve a distinct purpose and hold proper authority over relevant stakeholders and decisions. Lack of clear distinction between each entity regarding their authority and responsibilities may result in inefficient use of resources through duplicated efforts, failure to implement privacy requirements through diffusion of responsibility, or conflict between entities due to perceived breaches of authority.

3) Policies require a written data governance plan and processes.

Without written plans and processes, stakeholders may implement policies inconsistently throughout the state, as the policies may be subject to individual interpretation. Documentation of plans and processes also allows data governance policies and practices to be consistent through leadership or other personnel changes. Recording informal plans and processes in an easily understood form is challenging but can also reveal gaps or redundancies that need to be addressed. When plans and processes are informal and depend on specific individuals, not defined roles, data governance implementation may be inconsistent, inadequate, and inefficient.

Essential characteristics of an effective data governance program include the following:

- Creating privacy policies that protect 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;
- Ensuring that education stakeholders understand which data is protected, 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;
- Providing accountability and transparency through clear documentation of roles, policies, and procedures and through continuous engagement with education stakeholders.

The state of Maryland public institution higher education privacy law enacted in 2020 includes privacy governance program characteristics like the ones outlined above. The law requires institutions to identify why they are processing student personally identifiable information, prohibit re-disclosure of personally identifiable information except when certain circumstances apply, and implement fair information privacy practices that include data subject access rights.[74] The law's specification of the basic elements to be included in a public institution's privacy governance program ensures that all students at the state's public higher education institutions have similar basic protections with respect to their data. Additionally, Illinois has a distinct policy surrounding SLDS data, with specific requirements for the state Department of Education in collecting, maintaining and sharing it.[75]

II. STATE STUDENT DATA PRIVACY POLICIES

While Section I (State-level Commitment to Student Privacy) answers foundational questions such as what the state is seeking to accomplish, which parties are involved, and who is tasked with carrying out responsibilities, Section II describes how to build on this foundation. To make a state-level commitment to student data privacy actionable, there must be policies established to support the commitment. Without establishing student privacy policies governing relevant parties, the state-level commitment will not be implemented. In this framework, policies are defined as any binding statutes, regulations, rules, or other mandates implemented by a governing body, such as a state legislature or school board. Policies may refer to a state privacy law, but more likely they refer to a regulation or state board resolution.

Policies also differ in the time needed and process required to implement or amend them. For example, amending a state law may require a lengthier process and more stakeholder involvement than what is involved in revoking a school board mandate. Regardless of the type of policy, the key is that student data privacy policies should be binding and impose clear obligations on parties who will access student data throughout the state. These policies will help education agencies and institutions, third-party vendors, and researchers understand the state's expectations with respect to safeguarding student data. Together, these policies will convey the state's overall approach to student privacy.

II. STATE STUDENT PRIVACY POLICIES

IIA. Develop and Implement Student Privacy Policies Governing Education Agencies and Institutions

1) Policies include clear definitions.

2) Policies provide clear instructions to education agencies and institutions while providing adequate flexibility so the agencies and institutions can tailor policy implementation to best suit their needs and context.

3) Policies ensure that data is collected only for specific educational purposes, that the data collected is limited to what is necessary for those purposes, and that the data is periodically reviewed to ensure that the data collection should continue.

4) Policies require education agencies and institutions to establish data use requirements and limitations that account for the following issues: how certain uses could contribute to or harm the well-being and/or educational success of an individual student or group of students; whether the use is fair and equitable; whether the underlying data is accurate; the original reason the data was collected and the reasonable expectations of the person from whom the data was collected; and prohibitions on the non-consensual use of student data for non-educational purposes.

5) Policies require education agencies and institutions to establish policies regarding access to student data.

6) Policies require that everyone who has access to students' personal information be trained and know how to effectively and ethically use, protect, and secure it.

7) Policies include data sharing limitations and requirements for education agencies and institutions, including clear, publicly available rules and guidelines for how both internal staff and third parties receiving data from education agencies and institutions can use, safeguard, share, or delete the data or collect additional data.

8) Policies require education agencies and institutions to periodically review the data they hold, delete or deidentify any data that is no longer necessary, and ensure that third parties with access to this information do the same.

9) Policies require that education agencies and institutions and their third parties examine potential impacts of data collection, use, sharing, and deletion on marginalized communities and implement safeguards to reduce the likelihood of bias and discrimination.

10) Policies restrict the sharing of student data with law enforcement except when a court order, subpoena, or other law compels such disclosure.

11) Policies require regular evaluation of agency and institutional compliance with student data privacy requirements and include measures for remediating incompatible practices.

12) Policies require education agencies and institutions to regularly assess third-party compliance with student data privacy requirements, and include procedures for remediating or eliminating incompatible practices.

13) Policies require ongoing reports to specified policymakers or public reports on education agencies' and institutions' implementation of student data privacy requirements.

1) Policies include clear definitions.
State policies should help education agencies and institutions understand their student data privacy requirements and responsibilities, and should create privacy guardrails around the collection, use, sharing, and retention of student data. To do so, policies should carefully define terms to establish common understanding among all stakeholders and clearly convey legislators' intent. Policymakers can mitigate unintended consequences by ensuring that legislative language is clear, specific, and reflects the contexts in which stakeholders will implement the laws. Without clear and specific language, the laws can be interpreted in various ways, which may result in confusion, anxiety, and unintended consequences. Moreover, when language is ambiguous, stakeholders may enact policies inconsistently, resulting in inefficiencies and potential conflicts with other laws. For instance, the term "data" can be interpreted in various ways. The law must therefore specify which types of data it refers to, how the policy defines the data, and the context from which that data comes.

In order to receive federal funds, states must comply with FERPA's definition of student data and other terms. While some states rely exclusively on federally mandated definitions of data, a 2015 report by the Foundation for Excellence in Education[76] concluded that 29 states have adapted their own definitions in their state laws in order to clarify and enhance state policy. For example, Colorado legislation includes different definitions of student data, education records, and personally identifiable information. Colorado also passed legislation whose impact is limited to only SLDS data. Similarly, Kansas legislation passed in 2014[77] differentiates student data, personally identifiable student data, biometric data, and directory information. Part 121 of the Regulations of the Commissioner of Education in New York, a law addressing K-12, opens with 20 unique definitions related to education data privacy.[78]

Similarly, "appropriate data use" is often subject to interpretation. What is appropriate may vary by community. Policies need to address this potential for divergent interpretations by establishing a narrow definition with limited exceptions as needed. An appropriate data use standard details the essential knowledge, skills, and professional behaviors required by those who access data to effectively inform instructional and programmatic decisions.

Since SLDS collect data beyond the public education system, the policy must require this data to be consistently governed, as it requires for all data elements. Policies should therefore clearly define public education data, to avoid ambiguity regarding which data is covered. Clear definitions also promote transparency for students and parents.[79]

2) Policies provide clear instructions to education agencies and institutions while providing adequate flexibility so the agencies and institutions can tailor policy implementation to best suit their needs and context.

Educational agencies and institutions should have the flexibility to improve their compliance process over time. Building a culture of privacy is an evolving process.[80] As a result, policies may need to change over time, causing a need for amendments not outlined in the original policy. Depending on the context, a need may arise for amendments not outlined in the original policy.Moreover, education agencies and institutions should have the flexibility to improve their compliance process over time.

In a 2014 report, EducationCounsel explained that while state policies should necessarily limit student data access to individuals with legitimate educational interests, policies should also "recognize varied local situations and evolving circumstances and therefore provide local school districts with sufficient flexibility to tailor solutions."[81] Essentially, there is no one-size-fits-all approach for who should have access to student data because educational purposes evolve. Just as policies that grant overly broad access to student data can be harmful, policies that are too restrictive may preclude uses of student data that can benefit students.

Throughout the framework, we identify points at which policies could allow education agencies and institutions and their third parties flexibility in carrying out objectives; establishing context, definitions, and values can help stakeholders ensure their practices align with the state's goals.

3) Policies ensure that data is collected only for specific educational purposes, that the data collected is limited to what is necessary for those purposes, and that the data is periodically reviewed to ensure that the data collection should continue.

Education agencies' and institutions' policies should establish appropriate limits on the use and repurposing of student data, to ensure that collection and use of student data is limited to purposes consistent with both education agencies' and institutions' relationship with students and the context in which the data was initially disclosed, unless required by law to do otherwise.[82] Policies should also ensure that stakeholders use student data only in ways that students, parents, and other stakeholders would reasonably expect. This means not using data in ways that could cause students harm or that they would find intrusive, assessing whether the data use is necessary and whether less-intrusive alternatives exist, and enacting safeguards to mitigate risks.[83] As the context of student data collection and use continuously evolves with new technologies, policies, and societal norms, education agencies and institutions should regularly review their data elements to assess whether the elements are still necessary to achieve defined goals.

Without these safeguards, education agencies and institutions expose themselves to unnecessary risk of data misuse or breaches. Limiting the student data collected and retained also minimizes these threats. For example, collecting and retaining students' immigration statuses may put students and their families at risk of deportation if Immigration and Customs Enforcement (ICE) issues warrants or subpoenas to access these records. If collecting this information is not in the students' best interests, education agencies and institutions should consider not collecting the data.

Policies should also consider requiring the definition of categories of data that education agencies and institutions may or may not permissibly store, based on the type of institution holding the data. For example, policies may allow local education agencies to house certain sensitive information, such as an individual student's biometric information (e.g., a fingerprint used for school lunch purposes), while prohibiting state education agencies from housing the same data. Policies can also implement the use of data governance systems as means for educational institutions to keep track of the data that they maintain, and ensure that only necessary data is being collected. Part of data governance is knowing what data is collected and its purpose, which can be fulfilled through a "data inventory." Data inventories usually provide a list of the data elements collected and the rationale for collecting those elements. While federal law does not require the use of data inventory systems among educational institutions, and state laws vary in their requirements, such systems can be helpful tools for governments to determine what data is being collected and for what reasons. Oklahoma's 2013 student privacy law (HB1989) mandated the creation of such an inventory, which also must include the purposes of collecting each data element.[84] A similar law was passed in Tennessee.[85] Other requirements for the data inventory may include (a) the statutory or regulatory authority for data collection; (b) purpose of data collection; (c) length of time that the state or federal authority holds that data; and (d) tasking the educational agency or institution with developing protocols for the storage, destruction, or archiving of data or a collection.

Education agencies and institutions may enact such policies by establishing a protected public data inventory that lists the data elements collected by the state and federal governments, including the SLDS, and the rationale for collecting those elements. A state bill in Oklahoma (HB1989) mandates the creation of such an inventory, which also must include the purposes for collecting each data element.[86] Similar legislation exists in Tennessee.[87] Other requirements for the data inventory may include the statutory or regulatory authority for data collection, purpose of data collection, length of time that the state or federal authority holds the data, and tasking the education agency or institution with developing protocols for the storage, destruction, or archiving of data or a collection.

Policy should also identify the location of the data inventory or require the state agency/institution to house the inventory in a prominent, accessible location. In either case, the purpose is to ensure that the data inventory is both easily accessible in a public, online location and prominently featured on the site. A data inventory should not be hidden or require many clicks within a website. Websites should have navigation menus that include a section indicating where to find data practices and student privacy

information. If possible, a single page or section of the website should consolidate information on data practices and privacy. At the SLDS level, Colorado's SchoolView is a laudable example of public transparency regarding the state's student data collected and maintained.[88] The website provides text and visual information on data elements across the state, such as student enrollment, principals' effectiveness ratings, and course offerings.[89]

Policies should also allow input from the education data and oversight governance board, agencies, institutions, and a diverse group of qualified stakeholders to determine which elements should be included, the process for selecting those elements, and how those elements should be used. The policies may also define which student data can and cannot be collected at the state or district level. For example, facial recognition could be a type of data that cannot be collected. Convening a diverse group can alleviate concerns about data misuse because the process is collaborative, rather than a small group making decisions on behalf of the state.[90] For example, leaders of Washington's Education Research and Data Center[91] meet several times with stakeholders relevant to data sharing, spending nearly eight months to develop processes and expectations and to alleviate concerns.[92] At the SLDS level, Michigan's Center for Educational Performance and Information not only provides a public spreadsheet outlining all of the data elements collected by the state,[93] but they also indicate the purposes for the data collection. These purposes include school funding, transparency, accountability and compliance with state and federal laws, informing educational policies and practices, and state and federal reporting.[94] Additionally, Maryland Senate Bill 375 established an SLDS governing board of appointed individuals, including those in state-level positions and those in local districts.[95] The bill indicates responsibilities specific to the governing board to maintain the SLDS. Both New York[96] and Ohio[97] have a similar governing body comprising a diverse group of representatives from the state.

4) Policies require education agencies and institutions to establish data use requirements and limitations that account for the following issues: how certain uses could contribute to or harm the well-being and/or educational success of an individual student or group of students; whether the use is fair and equitable; whether the underlying data is accurate; the original reason the data was collected and the reasonable expectations of the person from whom the data was collected; and prohibitions on the non-consensual use of student data for non-educational purposes.

Student data is instrumental in defining educational goals and priorities and in properly allocating and distributing resources to achieve those goals. For example, disaggregated data on student graduation rates may reveal lower rates among Black or Brown students or students experiencing homelessness, which may prompt greater investment in supplementary support systems for those student groups. However, student data may also be used explicitly or implicitly to harm students from underserved communities. For instance, when improperly shared with law enforcement, a student's household income or disciplinary record may be used for predictive policing programs that identify vulnerable students as future criminals and increase police presence in their communities.

Keep in mind that data collection and processing may reinforce human biases in a manner that further marginalizes and harms the most vulnerable people. Recognizing the unfair distribution of risks and benefits of data use across a community is a critical step in developing student privacy policies that do not reinforce societal biases, disguise prejudiced decision-making, and block equal opportunities for marginalized or vulnerable populations.[98]

Given the particular, exacerbated privacy risks for students from underserved communities, policies should require education agencies and institutions to prioritize fair and equitable data use that is in each student's best interests. Education agencies and institutions should also seek to rectify inaccurate, incomplete, or biased data. Data-driven decisions are only as good as the underlying data informing the decision-makers. The Colorado Department of Education's website acknowledges this by stating, "Decisions are only as good as the data on which they are based,"[99] demonstrating that the state prioritizes data integrity. For these reasons, maintaining the accuracy, completeness, and fairness of data should be a priority.

5) Policies require education agencies and institutions to establish policies regarding access to student data.

Education agencies and institutions should allow access to student data only to those who need the data to support their professional duties. Moreover, access should be limited to only the data necessary to complete defined tasks. While a school administrator may have a legitimate educational need to access some information about students, their job probably does not require access to all of the student data that the school maintains. This is especially true in higher education settings. For example, a university's medical center likely does not need access to a student's academic records, just as professors probably do not need access to a student's health records.

Data minimization is a core principle in the "Student Data Principles" signed by 41 education organizations, such as the School Superintendents Association (AASA), American Federation of Teachers (AFT), National PTA, and the Council of Chief State School Officers: principle eight recommends that "educators and their contracted service providers should only have access to the minimum student data required to support student success."[100] In their 2014 report, Education Counsel describes a Maryland statute that limits access to the state's longitudinal data system, as an example of a statute that incorporates access safeguards.[101] Delineating and assigning levels of access helps mitigate the risks of unauthorized disclosure and data breaches.[102] However, as previously explained, policies should also acknowledge the diversity of local contexts and evolving needs, to allow school districts to adapt and tailor solutions to their unique needs and context.[103]

6) Policies require that everyone who has access to students' personal information be trained and know how to effectively and ethically use, protect, and secure it.

To ensure proper use and care of student data, anyone who has access to it should undergo training on how to effectively and ethically use, protect, and secure it. This is relevant to both the local and state levels. For example, in a K-12 school, teachers are immensely important to protecting student data privacy, as they make decisions daily that impact which student data is collected, how this data is used, and how data is interpreted to make decisions about students. Many educators are also unaware of the responsibilities they must uphold under FERPA, state privacy laws, and district and school policies that protect students' data privacy. For example, many teachers do not know they must use their district's app-vetting process before introducing a new edtech product into their classroom. If the district does not institute such a process, the app still must be properly vetted for privacy protections, or the educator must obtain written parental consent. As a result, teachers must receive training on why they should care about student privacy and their responsibilities under student privacy laws and district and school policies. Teachers should also receive training on basic data security, such as password management.[104]

An education institution that provides such training and shares it publicly is Eastern Michigan University, whose training covers the definition of PII, why it is important to protect it, which laws govern its use, and how to comply, among other topics.[105] At the SLDS level, North Dakota requires data protection training twice each year for anyone who has access to the statewide longitudinal data system.[106] Such frequent training ensures that stakeholders are up to date with technological changes, which occur rapidly. Wisconsin's Department of Public Instruction has an approval process for granting SLDS data access for training purposes that includes timeframe limits and a data confidentiality agreement.

Training must also be ongoing to ensure that educators and individuals with access to student data develop data literacy skills and receive updated information on the latest trends and best practices. As the Data Quality Campaign explained,

> For educators to make data work for students, they need training and guidance on data use–both at the start of and throughout their careers. To the extent that state policies have been used as a tool to provide these critical supports in recent years, the efforts have focused more on privacy and security training than on more comprehensive data literacy skills educators need to use effectively and ethically.[107]

7) Policies include data sharing limitations and requirements for education agencies and institutions, including clear, publicly available rules and guidelines for how both internal staff and third parties receiving data from education agencies and institutions can use, safeguard, share, or delete the data or collect additional data.

Since third parties of the state may access personally identifiable information, they should also be responsible and held accountable for protecting the privacy of student information. Without this requirement, PII could fall into the hands of an actor who is not prepared to manage it appropriately. More than 30 states have enacted student privacy laws that directly regulate vendors and third parties that receive student data, requiring these third parties to abide by and be held accountable for instituting specific student privacy safeguards.[108] For example, a proposed Texas bill requires operators that do business with local education agencies to adhere to the data protection requirements established by the agency.[109] The Texas statute designates specific purposes for which third-parties may use student information[110] as well as those they are prohibited to engage in.[111]Additionally, California's Education Code grants school districts the right to audit and inspect vendors' compliance with relevant privacy contracts.[112] Additionally, education agencies and institutions should institute policies that limit data sharing within the institution, ensuring that only actors who require particular student information can access that information for the appropriate time period. For example, a librarian who does not interact with a particular student should not be able to access that student's IEP.

To assess the implementation of this element, education agencies and institutions must ask whether policies require contractors, vendors, legitimate educational actors, and any other third parties of state or local agencies and institutions to safeguard student data, and they must hold these third parties accountable for complying with these requirements. Education agencies and institutions should also communicate to third parties the requirements and expectations for security and privacy standards.

8) Policies require education agencies and institutions to periodically review the data they hold, delete or deidentify any data that is no longer necessary, and ensure that third parties with access to this information do the same.

Education agencies and institutions should conduct regular reviews to ensure that data collected is always for a necessary purpose. This keeps the data governance plan from becoming stagnant and outdated. If data is no longer necessary, it may be appropriate to deidentify it. Deidentified data refers to data through which a link to any individual cannot be established.[113] Deidentification is a key method for ensuring privacy during data processing. Although PII can be traced to an individual, incorporating requirements for deidentification as a use-limitation measure protects privacy and gives state agencies guardrails within which to operate.[114] Although not identifiable, deidentified data can still be traced to a person's identity if a data characteristic is uncommon and/or data elements can be connected to build a recognizable identity. Thus, stakeholders should still handle deidentified data with care. Since deidentified data can be linked to an individual if a data point is rare, Washington state requires that data aggregated from fewer than 10 individuals be suppressed to protect individual privacy.[115]

Regarding deletion, the US Department of Education's Privacy Technical Assistance Center (PTAC) has released a best practices guide for data destruction, including general recommendations and methods for destruction.[116] While FERPA does not require data destruction, the Department of Education recommends it in order to balance the large amount of data collection in schools and to minimize the possibility of a digital permanent record. Some states, such as Kansas, have instituted guidelines for data retention that go beyond what data sharing agreements require or when an agreement expires (whichever occurs first).[117]

In some cases, data may need to be archived. Stakeholders should clearly articulate these cases as exceptions and should store data in a secure location. One example is Utah's publicly available Records Appraisal & Management Program (UTAH RAMP), which applies to LEAs and the Utah State Board of Education. UTAH RAMP is a records-retention schedule that provides guidance regarding which records should be preserved.[118] School districts can follow the retention schedule in entirety, can follow a modified version, or they can adopt

their own retention schedule as the law permits. Data retention and deletion are essential, as a mistake from elementary school, later taken out of context, should not follow students throughout their educational journey.[119] Particularly, education stakeholders should not track and store students' browsing patterns as it is not only unnecessary to schools' functioning but may also discourage students from researching topics that schools may consider unacceptable but would significantly aid students.

9) Policies require that education agencies and institutions and their third parties examine potential impacts of data collection, use, sharing, and deletion on marginalized communities and implement safeguards to reduce the likelihood of bias and discrimination.

Data collection, use, sharing, and deletion may have unique, negative impacts on marginalized communities. For example, an investigation in 2020 revealed that some universities used race as a factor in determining whether certain students were at risk of failing or dropping out of school, reporting that universities categorized Black students as "high risk at as much as quadruple the rate of their White peers."[120] Students categorized as high risk are subject to more interventions and steering, which can dissuade students from pursuing careers in their chosen fields. Education agencies and institutions should ensure that their data practices do not harm the students they intend to serve, especially students living in poverty, students with disabilities, students learning English as a second language, students experiencing homelessness and the foster care system, students who are incarcerated, undocumented students, Black and Brown students, Native students, Asian students, students who identify as LGBTQ, as well as students who experience multiple vulnerabilities.[121]

However, education agencies and institutions should note that data can also be a powerful tool for exposing such harms. For example, using student test scores, disciplinary data, and data on biases, a 2020 study found that "teachers' implicit biases may have an impact on student outcomes," as the study connected "county-level teacher implicit bias to disparities in achievement and school discipline between Black and white students at the county level."[122] For any education data initiative, education agencies and institutions should institute processes for identifying any risks to their students, particularly students experiencing vulnerabilities, and introduce safeguards to account for those risks.

10) Policies restrict the sharing of student data with law enforcement except when a court order, subpoena, or other law compels such disclosure.

In certain circumstances, education agencies may receive requests to share student data with law enforcement. Policies should clearly restrict education agencies' disclosure of student data to law enforcement to lawful requests, such as a court order, subpoena, or an event that triggers another applicable exception to FERPA's consent requirement, such as a health or safety emergency.[123] Education agencies should be cautious about sharing student data with law enforcement agencies. Moreover, policies should clearly dictate the appropriate legal and procedural steps that education agencies and institutions should follow when responding to law enforcement requests, including the appropriate methods for documenting requests and limiting impermissible secondary uses or redisclosures. Education agency and institution staff should know the appropriate points of contact, such as legal counsel, for routing such requests. Education agency and institution staff must also know the permissible distinctions between sharing student data with school-employed law enforcement, such as school resource officers, and external law enforcement bodies.

11) Policies require regular evaluation of agency and institutional compliance with student data privacy requirements and include measures for remediating incompatible practices.

Audits are necessary to maintain accountability and compliance with policy. The responsibility for requesting these audits rests with the state privacy leader, as they oversee and delegate responsibilities. Through annual monitoring, the state privacy leader can ensure that all education agencies and institutions adhere to required data governance policies and update them as technology advances and data access and limits evolve. For example, evaluations of data use, security, control, and privacy should occur. These audits should occur regularly not only for education agencies and institutions but also for contracted third parties with access to student data.

12) Policies require education agencies and institutions to regularly assess third-party compliance with student data privacy requirements, and include procedures for remediating or eliminating incompatible practices.

Establishing mechanisms for evaluating compliance is an administrative safeguard to protect privacy. State agency and institution practices should be evaluated to ensure compliance, and policies can be enhanced if necessary. Incorporating the step of evaluating compliance ensures that privacy is always top of mind because it is an evolving process. Establishing consequences for noncompliance encourages state agencies and individuals to always act with care to follow the established privacy practices.

13) Policies require ongoing reports to specified policymakers or public reports on education agencies' and institutions' implementation of student data privacy requirements.

Regular reports inform policymakers and relevant stakeholders of the successes and challenges of policies, thereby helping to modify policies or develop new ones in order to address evolving student privacy needs and risks. The reports also encourage internal accountability within education agencies and institutions as they compile and curate information for the reports, potentially addressing gaps or inefficient processes and practices prior to external review.

IIB. Establish Student Privacy Policies Governing Third-Party Vendors

1) Policies require third-party vendors to enter into written agreements with education agencies and institutions before the vendors receive student personal information.

2) Policies restrict third parties from collecting, using, retaining, or sharing student data for noneducational purposes, including selling the data and building student profiles to inform advertisements.

3) Policies limit the student data available and/or provided to third parties to the minimum data required to fulfill their duties.

4) Policies require third parties to be transparent about data collection, use, sharing, retention, and storage.

5) Policies require third-party employees who receive student data to undergo training that ensures they know how to responsibly, ethically, and equitably use, protect, and secure student data.

6) Policies establish penalties for third parties that fail to comply with student privacy requirements.

1) Policies require third-party vendors to enter into written agreements with education agencies and institutions before the vendors receive student personal information.

> "A local or regional board of education shall enter into a written contract with a contractor any time such local or regional board of education shares or provides access to student information, student records or student-generated content with such contractor." Conn. Gen. Stat. § 10-234bb (2018)

When an education agency or institution seeks to form a partnership with a company that provides educational technology, the parties must agree to written terms regarding the use of PII. Education agencies and institutions must ensure that any third party with whom they share PII is contractually obligated to treat it in alignment with the agencies' and institutions' own privacy standards. In some cases, education agencies and institutions may want to share personal information with companies that have

tools that were not developed for the education context. For example, during the shift to online learning necessitated by COVID-19, schools conducted remote classes by using video conferencing solutions that were often built for corporate uses. In these cases, written agreements are especially important to make sure the third party understands the unique privacy protections that apply to student data but not to general consumer data. For these and other reasons, several states require that third parties enter into written agreements with education agencies before receiving student data, including but not limited to Connecticut, Idaho, and Kansas.[124]

2) Policies restrict third parties from collecting, using, retaining, or sharing student data for noneducational purposes, including selling the data and building student profiles to inform advertisements.

Policies should restrict third parties from using student data for noneducational purposes and/or what the written agreement prohibits, including the creation of student profiles to inform advertisements. Among states in which student privacy laws enumerate required contract terms, Kansas and Missouri specify that contracts include the purpose of the agreement and limit the use of student data to those parameters.[125] Beyond contractual requirements, federal and state student privacy laws usually prohibit third parties from building student profiles for advertising and from practicing targeted advertising.[126]

3) Policies limit the student data available and/or provided to third parties to the minimum data required to fulfill their duties.

When education agencies and institutions cannot fulfill a need, they often use third parties. Third parties should receive only the minimum amount of student data required to complete the agency or institution's needs, in alignment with the Fair Information Practice Principle of data minimization, which directs entities to collect only PII directly relevant and necessary to accomplish a specified purpose and to retain the PII only for as long as necessary to fulfill the purpose.[127]

4) Policies require third parties to be transparent about data collection, use, sharing, retention, and storage.

To build trust regarding student data's life cycle, policies must inform stakeholders of how and why data elements are collected to ensure that education partners know and can communicate how student data is used within the third party's platform, and to ensure appropriate limitations regarding the use of student data. Policies should also state how data may or may not be shared with parties beyond a given third party. Both data subjects and institutions should know how long a third party will keep their data and the methods used for its proper storage. For example, New York requires education agencies to publish on their websites information about contracts with third parties that receive student PII. Required information includes the types of PII that contractors receive, the terms of the contracts, subcontractors that the contractor intends to use, and more. To meet this requirement, third parties must submit the information to the education agency as a part of the contracting process.[128]

5) Policies require third-party employees who receive student data to undergo training that ensures they know how to responsibly, ethically, and equitably use, protect, and secure student data.

> "Such plan shall include a requirement that any officers or employees of the third party contractor and its assignees who have access to student data or teacher or principal data have received or will receive training on the federal and state law governing confidentiality of such data prior to receiving access."
> N.Y. EDUC. LAW § 2-D

Policies should ensure that any individual who can or does access student data undergoes applicable and context- and role-specific student privacy training. Those actors should fully understand how to appropriately safeguard student data within their roles as well as appropriate limitations on its use and disclosure—not just in compliance with policies but also consistent with ethical and equitable uses. Some states have enacted legislation or regulation to require third parties to undergo training; in New York, third parties must outline

in their contracts with education agencies how employees and assignees who access student data will be trained on the relevant laws governing the data, before they receive access.[129]

6) Policies establish penalties for third parties that fail to comply with student privacy requirements.

To promote compliance and maintain accountability, any actor who fails to comply with student privacy safeguards regarding both security and ethics should be subject to clearly defined penalties. Unless actual enforcement exists, actors may feel that they can get away with mistreating or misusing students' information. Policies unaccompanied by enforcement are often ignored. Under FERPA, violations may result in withdrawal of federal funding. However, the US Department of Education has not exercised this tool, so this penalty still lacks teeth to enforce compliance. Policies should explicitly state reasonable enforcement actions and should allow entities tasked with enforcement to conduct investigations and determine appropriate fines or sanctions for noncompliance. One such policy is California's Student Online Personal Information Protection Act (SOPIPA). As a Common Sense Media report explained, "SOPIPA is enforceable directly against companies. This can make it a more effective tool in protecting student privacy than FERPA and laws only enforceable against schools."[130] Establishing actual consequences for violating student privacy policies can reinforce the great responsibility that comes with accessing student data and ensure that third parties take the right steps to safeguard student information.

IIC. Establish Student Privacy Policies Related to Researchers

1) Policies direct education agencies and institutions to develop approval criteria for researchers' requests to share data, to balance the potential value and benefits of the research with privacy risks.

2) Policies establish best practices and guidelines for researchers to safeguard student data privacy.

3) Policies recommend or require researchers to be trained not only in human-subjects research but also in student data privacy compliance and best practices.

4) As appropriate and/or applicable, policies recommend that education researchers have a clear privacy statement or policy on their website and discuss with research subjects the guidelines that researchers and their organizations follow when using student data.

5) Policies require that any report resulting from data obtained via requests include only deidentified or aggregated information.

1) Policies direct education agencies and institutions to develop approval criteria for researchers' requests to share data, to balance the potential value and benefits of the research with privacy risks.

Restrictions on sharing student data with researchers help the state manage data-access requests, including requests for access outside the scope of what the state deems appropriate. Texas's Education Research Centers (ERC) provide researchers access to up to 30 years of longitudinal SLDS data if the researchers undergo a process that, among other requirements, determines whether the research needs the requested data elements to answer the research questions.[131] All research that the ERC approves must be for "the benefit of Texas," must be completed at an ERC, and the researcher may not leave the facility without review by the ERC staff to ensure FERPA compliance.[132]

2) Policies establish best practices and guidelines for researchers to safeguard student data privacy.

Because researchers will have access to student data, they should be held to high standards to safeguard student privacy, similar to the way that policies establish standards for education institutions at all levels of the state. Clearly articulated policies should establish these standards. Articulating best practices and guidelines for researchers is important to ensure that school communities can trust that their data will be

protected.[133] While hackers may not find student data collected for research purposes more appealing than other types of data, it is important to acknowledge the harms that could arise from any data disclosures as well as public perception of student data exposure.[134] Providing best practices and guidelines for researchers shows that policymakers have considered these potential harms and are acting thoughtfully to mitigate risks.

3) Policies recommend or require researchers to be trained not only in human-subjects research but also in student data privacy compliance and best practices.

Given the sensitive nature of student data, researchers who access the data should first prove that they have completed human-subjects training, such as the Collaborative Institutional Training Initiative (CITI), which is federally mandated for researchers who submit a proposal to the institutional review board (IRB). The IRB's standards and rigor should apply to research that involves interaction with human-subjects data, including deidentified data. While training such as CITI covers ethics and responsible research practices, it does not address state laws concerning data use or data security. Furthermore, because it applies to any human-subjects research, it does not cover the context-specific training necessary for handling student data. Therefore, a panel at the National Academy of Education has recommended that education researchers complete not only standard human-subjects research training but also training on student data privacy.[135] Moreover, researchers should be prepared to communicate the value of their research to relevant stakeholders.

4) As appropriate and/or applicable, policies recommend that education researchers have a clear privacy statement or policy on their website and discuss with research subjects the guidelines that researchers and their organizations follow when using student data.

Researchers who use student data for their work understand that the data is particularly sensitive. As a result, they should proactively communicate the purpose of their research and how it will benefit the community. They should also explain how they are qualified to manage student data, from proper storage to eventual destruction methods. The National Academy of Education has emphasized transparency regarding researchers' practices, including who has access to the data and for what purpose.[136]

5) Policies require that any report resulting from data obtained via requests include only deidentified or aggregated information.

In some instances, relevant parties may wish to use student data in their public reporting, including in research publications. However, policies must institute processes to protect student data privacy before publication, specifically by requiring the data to be deidentified or aggregated. Policies should ensure that agreements with and within education agencies and institutions include this requirement.

Policymakers must also consider that data deidentification and aggregation techniques are not a silver bullet. Computer scientists continue to develop methods for reidentifying data, and future data sets may allow previously deidentified information to be linked to individuals.[137] Nonetheless, data privacy experts Jules Polonetsky, Omer Tene, and Kelsey Finch state that "de-identification techniques unlock value by enabling important public and private research, allowing for the maintenance and use—and, in certain cases, sharing and publication—of valuable information, while mitigating privacy risk."[138] Such policies must be nuanced, allowing flexible, risk-based approaches to deidentification standards that allow researchers to use important student data, while reflecting the importance of deidentification or aggregation for mitigating privacy risks. Furthermore, such policies should help stakeholders understand that sharing data at the aggregate level minimizes unintended information disclosures and can further enhance public trust in agencies and institutions.

III. EDUCATION AGENCY AND INSTITUTION PRIVACY REQUIREMENTS

While this framework focuses on privacy practices, it is important to acknowledge the role of security in a privacy framework. Data security protects the confidentiality, integrity, and availability of data through various security practices, such as implementing technical, administrative, and physical safeguards. Data security helps to protect student data but cannot, by itself, sufficiently protect student data privacy. Therefore, education agencies and institutions must develop and articulate policies and processes that comprehensively address both data security and data privacy.

As explained above, the state must articulate clear privacy commitments and standards regarding data. However, flexibility is important for education agency and institution privacy requirements. Because education agencies and institutions are the parties that support implementation of the state's student data privacy commitments and policies, the agencies' and institutions' processes, procedures, and data needs may evolve over time. Allowing these parties to set some of their own privacy requirements ensures that policies do not become stagnant and outdated. For example, training may need to change to reflect new policies or be refined based on stakeholders' feedback. Creating a culture of privacy is an evolving process, and stakeholders should evaluate and improve requirements over time. While education agencies and institutions should have the flexibility to develop and articulate their student data privacy policies and processes, state policies should mandate standards and processes that achieve the state's goals. This creates consistency between what the state intends and what education agencies and institutions practice.

1) Policies require that education agencies and institutions write student data privacy and/or data governance plans that include administrative, physical, and technical safeguards.

To ensure data privacy, policies must address the security of the data. Security measures should have appropriate administrative, physical, and technical safeguards to protect data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. Administrative safeguards address the administrative level of a data governance plan, such as training for employees and contractors. An education institution that provides such training is Eastern Michigan University, whose training covers the definition of PII, why it is important to protect it, which laws govern its use, and how to comply, among other topics.[139] At the SLDS level, North Dakota requires data protection training twice a year for anyone who has access to the statewide longitudinal data system.[140] Such frequent training ensures that applicable stakeholders are up to date with technological changes, which occur rapidly. Physical safeguards address the physical features that protect data, such as locking doors in locations where data is stored. Technical safeguards address the technology used to protect data, including computer firewalls and restricting access to data to certain users.

2) Policies direct state or regional agencies (as applicable) to develop and regularly update or supplement model student data privacy policies and training resources that local agencies, including school districts, schools, public early childhood programs, and postsecondary institutions, can use.

The state should provide model data privacy policies and training resources to local agencies because schools often do not have the resources to do so. Furthermore, schools should not have to reinvent the wheel given that state agencies and institutions can create resources that apply throughout the state. For example, the Idaho State Board of Education created a model student data privacy and security policy for schools.[141] In Connecticut, members of the Data & Privacy Advisory Council of the Connecticut Commission for Educational Technology created a toolkit to help school districts with the rollout of Connecticut's student privacy law. Acknowledging that school districts are often the parties implementing policies, the toolkit provides resources for best practices and guidance as districts worked to comply with the new law.[142]

3) Policies require that education agencies and institutions develop and communicate appropriate student data privacy onboarding and offboarding protocols for employees and third parties.

Onboarding employees and contractors is particularly important to ensure that employees and contractors are trained in security protocols, know how to appropriately handle data, and engage in responsible and ethical data practices. Offboarding employees and contractors is another critical step to prevent unauthorized access. A Massachusetts state law applying to all people who own or license personal information about Massachusetts residents imposes minimum security requirements, including preventing terminated employees from accessing records containing personal information.[143] While this law does not target education agencies or institutions, it illustrates the types of administrative, physical, and technical safeguards that can protect data.

4) Policies recommend measures that foster education agencies' and institutions' ongoing commitment to safeguard student data privacy.

For student data privacy efforts to succeed, education agencies and institutions must have policies that foster a sustained commitment to student privacy. Such policies should thread student data privacy considerations through the educational ecosystem, rather than view this privacy as a compliance issue. Holding student data privacy protections as an agency or institutional value or priority ensures that appropriate attention and resources are available to support student data privacy initiatives.

5) Policies require education agencies and institutions to write a public process for community input regarding substantive changes to or new student data collection, use, sharing, or retention practices.

Education agencies and institutions should clearly communicate a process for stakeholder input. To encourage community feedback, specific processes should exist for community members to voice their concerns regarding data policies. Ideally, there should be a single channel for providing input so that stakeholders are not overwhelmed with input from various channels. Furthermore, providing information about the law on the public-

facing website allows community members to understand what they can and cannot change regarding data collection policies, as student data privacy laws require or prohibit certain processes.

6) Policies require that education agencies and institutions and their third parties work to ensure algorithmic fairness and to mitigate risks of bias from data systems, and report their efforts in this area.

Algorithms used for decision-making involve inherent bias because algorithms depend on the assumptions made from a set of training data (previously collected data used to make predictions). As a result of this biased input, algorithms can produce biased output.[144] While organizations increasingly rely on data to automate their decision-making, bad data can lead to bad policies. Even individuals not directly represented in a data set may be impacted by biases in the data set or analysis performed on it. Conclusions drawn from this data may adversely affect students who attend schools that underperform, and the students may be subject to bad policies implemented as a result of those conclusions.[145] Policies should consider these potential harms by requiring education agencies and institutions and their third parties to ensure algorithmic fairness so that data is used in a beneficial, productive way. Additionally, the FTC recently signaled that unfair or biased algorithms may violate Section 5 of the FTC Act.[146] This could mean that in the future, unfair or biased algorithms could be subject to FTC enforcement. Regardless of potential legal implications, policies should make it a best practice to mitigate risks of unintended consequences resulting from unfair algorithms and to report efforts.

7) Policies recommend or require that education agencies and institutions conduct regular assessments or analyses of the privacy impacts of data collection, use, sharing, and retention that balances the benefits of the data practices with associated student privacy or equity risks.

Assessments are important because they determine whether state agencies and institutions fulfill requirements. Audits can confirm that data is collected and processed in accordance with laws or policies. While there are numerous ways to audit processes, data holders may consider conducting a privacy impact assessment to identify and mitigate privacy risks. Policies may either prescribe a schedule for conducting audits or allow agencies and institutions to create their own schedule of regular audits. For example, the Department of Homeland Security conducts a privacy impact assessment when developing or procuring new systems that collect PII, creating a new program or system that may have privacy implications, updating a system that results in new privacy risks, or engaging in rulemaking that involves PII collection.[147] A postsecondary institution that implemented an audit process is the University of Washington. In 2020, the university formed a task force to inventory, map, and assess all of the university's personal data processing activities.[148] In addition to developing and updating university policies and standards related to privacy, the task force developed a privacy impact assessment form for departmental use, as well as providing the applicability under which to complete a privacy impact assessment.[149]

IV. A STATEWIDE TRANSPARENCY PLAN

As Section I mentioned, the use of student data involves the perception of competing values. There is value in protecting students' privacy and limiting data use, but the use of student data to produce beneficial outcomes for students and stakeholders may suggest a competing value. A statewide transparency plan is essential for addressing these competing values because individuals and communities will routinely have questions and concerns about how their information is being used. Education stakeholders should create and effectively communicate a statewide transparency plan to create legitimacy and public trust in data initiatives and research. Because stakeholders use data for the benefit of the community, they are obliged to be transparent and inclusive by ensuring that the community's concerns are heard and addressed. The community should be able to publicly access information regarding policies and should have opportunities to be heard. Moreover, because education stakeholders collect data from various parties and use it for many purposes, the statewide transparency plan should be comprehensive enough to include all relevant parties in the data process, including third parties and staff at education agencies and institutions, so that information is communicated through all appropriate avenues. Additionally, the statewide transparency plan should be maintained to account for policy developments and stakeholder feedback. Transparency is key to creating and maintaining an evolving culture of privacy throughout the state.

IV. Statewide Transparency Plan

1) Policies require education agencies and institutions to designate point(s) of contact for students, parents, staff, third parties, community members, or other appropriate stakeholders to communicate with and raise questions or concerns regarding agencies' and institutions' student privacy and data governance practices.

2) Policies require education agencies and institutions and their third parties to explain how their data security and privacy practices comply with FERPA and associated state privacy laws.

3) Policies ensure that the state, education agencies and institutions, and their third parties provide public information regarding the PII that they collect.

4) Policies require education agencies and institutions to provide easily accessible information to education stakeholders, including students, parents/legal guardians, and the public, about proposed significant student data initiatives, their purposes, and the policies and processes underlying data collection, use, sharing, protection, and retention.

5) Policies recommend or require that education agencies and institutions post a public list of the third parties receiving student data.
(Optional: Policies require education agencies and institutions to publicly post data sharing agreements or other contracts that provide information about how student data will be collected, used, shared, protected, and retained, excluding information that could compromise the integrity or security of student data or third-party data systems.)

6) Policies recommend that education agencies and institutions train staff in how to communicate about student data use and privacy.

1) Policies require education agencies and institutions to designate point(s) of contact for students, parents, staff, third parties, community members, or other appropriate stakeholders to communicate with and raise questions or concerns regarding agencies' and institutions' student privacy and data governance practices.

Designating point(s) of contact for communications is critical for transparency and accountability. Education agencies and institutions should clearly and regularly communicate point(s) of contact and their contact information through various channels. The point(s) of contact should respond to stakeholders in a timely and efficient manner, to assure stakeholders that their questions and concerns are a priority. Moreover, points of contact should understand the unique communications and communication methods relevant to each stakeholder. For example, students' questions and concerns may differ from those of a third party. The point(s) of contact should be well versed in student privacy and data governance; simply designating an individual without proper training, resources, or oversight is insufficient.

2) Policies require education agencies and institutions and their third parties to explain how their data security and privacy practices comply with FERPA and associated state privacy laws.

While state privacy policies vary, FERPA governs all of them. Relevant actors must transparently state how their practices adhere to applicable federal and state laws. The West Virginia Department of Education (WVDE) Data Privacy site includes easily accessible resources to learn about FERPA, the state's privacy law (the Student DATA Act), and the state's data privacy practices.[150] Community members can learn more about how FERPA and state laws protect student data, can access WVDE's Data Access and Management Guidance,[151] and can find a one-page resource on WVDE's mechanisms for protecting student data.[152] These documents explain how WVDE complies with privacy laws. Similarly, the Colorado Department of Education has developed a model website that outlines relevant laws and how they influence the agency's actions.[153]

3) Policies ensure that the state, education agencies and institutions, and their third parties provide public information regarding the PII that they collect.

Education agencies and institutions cannot prosper without the trust of their constituents. Trust establishes state agencies and institutions as responsible data stewards, but without trust in the programs, people may be inclined to provide false data, which would undermine the research process.[154] Individuals should be aware of how their data is used or not used, and it should not be hard to obtain this information. All collected data should not come as a surprise; rather, individuals should have consented prior to the information's collection and use.

State agencies and institutions have the power to provide information to affected individuals about collected PII. Data elements evolve over time. Therefore, it is appropriate for the policy to require that education agencies and institutions provide information on PII collected and to update the information regularly. Furthermore, state agencies and institutions should specify which elements are personally identifiable and which are collected in aggregate. If the public is informed about which information is collected, they can raise concerns through the appropriate channels, if necessary. This transparency also creates accountability in that the state collects no information outside the scope of what has been publicly revealed.[155]
Policies can recommend the creation of a public data inventory that lists all of the data elements the state collects, including (but not limited to) the elements collected by the SLDS, and the rationale for collecting those elements. The Utah Department of Education has a public-facing metadata dictionary that achieves this and categorizes data elements by the parties with whom the data is shared.[156]

4) Policies require education agencies and institutions to provide easily accessible information to education stakeholders, including students, parents/legal guardians, and the public, about proposed significant student data initiatives, their purposes, and the policies and processes underlying data collection, use, sharing, protection, and retention.

Providing easily accessible information is important for gaining community support and trust regarding student data collection. Consistent and open communication also helps to form a culture of privacy in each school.[157] This information includes data governance initiatives at the SLDS level. The Institute of Educational Sciences recommends communicating the value proposition of data governance to the community, including metrics and milestones that indicate data goals achieved.[158]

People in the community should feel that they have a voice regarding the handling of student data. If people cannot raise questions or concerns, trust in data initiatives will diminish. There should be opportuttnities for community members to raise concerns, such as at public meetings and through easily accessible online submission forms. Transparency is a key factor emphasized by the School Superintendents Association, which offers an example of a school district in Charlotte, NC that stressed the importance of listening to the community and collecting public feedback.[159] Metro Nashville Public Board of Education makes it easy for the public to participate in monthly board meetings, by providing clear directions on their website.[160] Not only can the public attend meetings, but meetings are also televised on a local cable channel.

There should also be ways to obtain meeting information for people who cannot attend. For example, Michigan's P-20 Longitudinal Data System Advisory Council provides a link to their latest meeting minutes on their website.[161] Providing minutes allows the public to understand what was discussed at a meeting, without needing to have direct access. This consideration ensures that all types of community members, regardless of their status, can be active in the student data privacy conversation.

5) Policies recommend or require that education agencies and institutions post a public list of the third parties receiving student data. (Optional: Policies require education agencies and institutions to publicly post data sharing agreements or other contracts that provide information about how student data will be collected, used, shared, protected, and retained, excluding information that could compromise the integrity or security of student data or third-party data systems.)

In the spirit of consistent transparency, state agencies and institutions should provide public information regarding their own data collection and should maintain an accessible list of the third parties who have

access to student data. The Utah State Department of Education's website[162] notes that education agencies and institutions should provide a comprehensive list of all third parties who have access to any state-level data. This promotes transparency and builds trust with the community. Connecticut's Department of Education has created such a repository of adopted applications from third parties.[163] By establishing this extra layer of transparency, education agencies and institutions demonstrate a commitment to informing the public about all aspects of student data.

6) Policies recommend that education agencies and institutions train staff in how to communicate about student data use and privacy.

In addition to training staff on data governance, education agencies and institutions should train staff on how to communicate about data use and privacy, particularly to people who are unfamiliar with the subject matter. Parents and students will have questions regarding student data privacy, especially given increased data collection and new technologies used with online learning. All staff should be prepared to answer related questions, but particularly teachers should be prepared as they are typically the first point of contact for parents who have questions or frustrations. Some high-level questions that staff should be able to answer involve technologies being used; the protections, security, and training that exist; parents' rights; and where parents can go to learn more. Families and students can feel overwhelmed or skeptical of edtech tools or how schools protect their children's data. Staff should be prepared to explain the specific benefits of using student data and edtech tools, how they enhance students' educational experiences, and the school's commitments to safeguarding student data. Staff must be trained on the decisions regarding student data so they can, in turn, have informed communication with others. Such communication builds and maintains trust and prevents confusion and misperceptions.[164]

V. RESPECT FOR STUDENTS AND THEIR DATA

As the Privacy By Design Foundational principles explain, stakeholders should design privacy practices with users in mind, to achieve the best results. Empowering individuals to manage their data can help prevent abuses and misuses of data. Respect in student data use means privacy policies that are human-centered, user-centric, and user friendly. This allows users to be adequately informed when making privacy decisions.[165] Inclusion and student agency and responsibility are two core elements of the Global Guidelines for Ethics in Learning Analytics. Inclusion ensures that stakeholders use data primarily to support students in student-centered ways, rather than focusing on the institution's needs and goals.[166] Similarly, state agencies and institutions should allow students to engage in policies and processes governing the collection and use of their data. Proactively engaging students can help ensure that data remains accurate and up to date, resulting in more-useful and fair data interpretations that are in students' best interests.[167]

The mission of the Ohio State University Privacy Program is to cultivate the community's trust that the university collects, uses, and shares personal information in a transparent, appropriate way. Using a privacy-by-design philosophy, the university's privacy principles include providing notice of data collection activities, honoring the data subject's choice about data collection activities whenever possible, making it easy for data subjects to access and correct their personal information, and securing information properly.[168] In 2020, the university strengthened campus outreach about privacy topics, convened its first privacy governance council, and launched several privacy working groups, including groups on student analytics and the privacy of minors.[169]

V. Respect for Students and Their Data

1) Policies require that students be free of harm, bias, or discrimination resulting from the use of their data, especially from algorithmic data used to predict outcomes.

2) Policies require education agencies and institutions and their third parties to use notice, choice, and consent mechanisms to allow students and parents to make legitimate requests for information about their data and to have control over its use.

3) Policies require that education agencies and institutions and their third parties clearly communicate to students and parents their rights and any methods of redress or correction of data in student records.

4) Policies require that educational agencies and institutions and their third parties clearly indicate to students and their parents the parties with whom their data is shared and the associated terms and security and privacy protections associated with data sharing.

5) Policies recommend that education agencies and institutions regularly solicit education stakeholders' feedback and recommendations regarding student privacy and data governance of new data initiatives or technology.

6) Policies require the creation of data literacy campaigns and curricula for students and families.

(1) Policies require that students be free of harm, bias, or discrimination resulting from the use of their data, especially from algorithmic data used to predict outcomes.

Requiring that students be free of harm, bias, or discrimination resulting from the use of their data ensures that data will be used in students' best interest. Unfortunately, there are many ways in which data can be biased and result in discrimination. For instance, stakeholders train facial recognition systems by using data sets composed predominantly of white male faces. Therefore, these systems identify darker skin tones, female faces, and transgender or nonbinary people far less accurately.[170] Adopting such a system may result in disproportionate harm to students of color or female students if they experience misidentification at a higher rate than their white male peers. Keeping students free of such harms reinforces the idea that stakeholders use data for students' benefit and in a student-centered way. This, in turn, helps promote people's trust in the state's data use.

The Electronic Frontier Foundation has created a resource for students regarding how one's privacy may be violated and how technologies can surveil individuals.[171] The content includes strategies for how students can best protect themselves from such invasions and unnecessary tracking.[172]

(2) Policies require education agencies and institutions and their third parties to use notice, choice, and consent mechanisms to allow students and parents to make legitimate requests for information about their data and to have control over its use.

Notice, choice, and consent are all essential mechanisms for ensuring that individuals are adequately and appropriately informed of data processing and collection practices. Without notice, an individual cannot meaningfully consent or contribute to the data process. Choice implies that individuals can opt in or opt out, rather than forcing individuals to participate in the process. Notice, choice, and consent work together to keep individuals engaged in the process and give individuals autonomy and control over their data. However, notice, choice, and consent mechanisms alone may be insufficient if students and parents do not fully comprehend what they are consenting to, due to the form in which the information is conveyed. Notice, choice, and consent mechanisms may also be insufficient if students' opportunities to engage in learning or activities is conditioned on use of certain tools. Therefore, education agencies and institutions should

ensure that underlying privacy protections accompany notice, choice, and consent mechanisms, and should address unintended impacts on students and parents who choose to opt out of certain data uses. Moreover, allowing opt-ins/outs in education is much more complicated than that outside of education. This is because data collection and technology use are generally involuntary in educational settings, and even when there is an option for parents or students to consent, they may not have all of the information to properly assess privacy risks and make informed decisions. Because opportunities for consent are limited in the educational context, notice and transparency are especially important, and the opportunities when there are opt-in or -out choices should be expanded when this would not interfere with essential school functions.

(3) Policies require that education agencies and institutions and their third parties clearly communicate to students and parents their rights and any methods of redress or correction of data in student records.

Schools must notify parents and students of their rights under FERPA. FERPA gives parents and students the right to correct data in their student records.[173] Parents and students may not be aware of their rights, so education agencies and institutions should clearly communicate this information so that individuals may exercise their rights if they choose. Understanding the rights that FERPA grants is particularly important for unaccompanied homeless youth, given that providing unaccompanied youth access to their own records removes barriers for enrollment and retention.[174] The US Department of Education has created a guide to help parents understand their children's rights under FERPA.[175]

In addition, accurate, complete, and unbiased data in an education data system is integral to helping stakeholders fully appreciate the benefits of student data. This is particularly true for longitudinal data systems that harness and build on data to design programs more effectively for student success. A report from Data Quality Campaign noted that data elements in a longitudinal data system cannot be successfully disaggregated if the data is not correct, assuming the state has a unique identifier to link data elements; for example, disaggregating incorrect test scores from special education data would make the data less useful.[176]

(4) Policies require that education agencies and institutions and their third parties clearly indicate to students and their parents the parties with whom their data is shared and the associated terms, security, and privacy protections associated with data sharing.

Informing individuals of the parties with whom their data is shared promotes transparency. Students and parents will receive accurate information, will be able to make informed decisions regarding their rights, and will more likely be engaged in the collection and use of their data. Because the state often contracts with third parties for various purposes, data can flow among the state, state agencies, and third parties. Empowering individuals with knowledge of security and privacy protections and their associated terms ensures transparency and instills confidence that their data will be protected. Increased transparency with students and parents can create more trust; otherwise, parents may be less inclined to support quality data processes.

Too often, stakeholders conflate transparency with availability. It is important that efforts to improve transparency consider the accessibility of information. For example, long privacy policies full of legal jargon may be publicly posted, but the intended audience is unlikely to read or understand the policy. In the same way, information about sharing student data with third parties and relevant terms and protections should be written so that students and parents can easily comprehend the information. The United Kingdom's Age Appropriate Design Code provides suggestions for communicating information about data use to young people in a transparent and age appropriate manner.

To date, few state laws have directly addressed transparency, although the Student Data Accessibility, Transparency and Accountability Act of 2013 requires that states publish the data elements they collect and demonstrate their compliance with FERPA.[177] The law also mandates that any new potential data elements and/or exceptions to the law be annually communicated to the state governor and legislature.[178]

5) Policies recommend that education agencies and institutions regularly solicit education stakeholders' feedback and recommendations regarding student privacy and data governance of new data initiatives or technology.

The creation of an intentional data governance system and development of a privacy-focused culture requires work from multiple stakeholders. These stakeholders must all be involved in the process as they have specific responsibilities and obligations to protect privacy, depending on their specific role and area of expertise. As parties implement policies, these stakeholders will have insight into how the policies and processes can be improved in order to meet the needs of their local community. To encourage this,policies should have mechanisms for soliciting recommendations that address unintended consequences, especially those that may disrupt teaching and learning, and avenues to iterate potential policy improvements. This includes opportunities for students, parents, legal guardians, and other community members to raise concerns and issues regarding such initiatives and processes. The solicitation of external input and feedback should begin during the policy development process and not exclusively once policy has been implemented. Seeking feedback during the policymaking process from a diverse group of stakeholders—including parents, students, third party contractors, ed tech companies, local and state agencies, and school districts—allows policymakers to identify gaps or unintended consequences that could result from proposed policies before they are implemented.

Education stakeholders can involve the public at various levels as appropriate to the student data privacy policy, practice, or issue. The following participation spectrum, adapted from the International Association for Public Participation, outlines five levels of public participation: inform, consult, involve, collaborate, and empower, which progress from least to most involved. This spectrum can help agencies and institutions determine how actively involved the public should be in each policy or issue:[179]

LEVELS OF PUBLIC PARTICIPATION GOALS	
Inform	To provide the public with balanced and objective information to help them understand problems, alternatives, opportunities, and/or solutions.
Consult	To obtain public feedback on analysis, alternatives and/or decisions.
Involve	To work directly with the public throughout the process to ensure that stakeholders consistently understand and consider public concerns and aspirations in decision-making processes.
Collaborate	To partner with the public in each aspect of the decision including the development of alternatives and the identification of the preferred solution.
Empower	To place final decision-making in the hands of the public.

6) Policies require the creation of data literacy campaigns and curricula for students and families.

Data literacy campaigns and curricula empower individuals to make informed decisions about their data. By teaching students and parents to be data literate, policies enact an overarching goal of data privacy, which is to allow students and parents to be engaged in their data collection and use. This also instills confidence in the process and shows that the state is working in students' best interest. For example, Metro Nashville Public Schools has implemented Student Data Chats[180] and Parent Data Chats[181] within their school communities. These chats give students a dedicated time to discuss their data with their teachers and principals in an accessible way, empowering students to use data to see where they are excelling and to set goals for improvement. During the Parent Data Chats, parents learn how and where they can access their children's data, how to interpret the data, and how to ultimately use the data to better support their children at home.

This element is specifically relevant to K-12 settings among both parents and students. Educating students and their families about student privacy and data literacy instills important knowledge and understanding early on.

VI. PROACTIVE PROTECTION OF STUDENT DATA PRIVACY

Sections I through V give specific policy recommendations for stakeholders seeking to pass responsible, ethical, and equitable student data privacy policies. This section, instead, provides suggestions for how policymakers can think through policies so that they prevent student data privacy issues and crises before they arise. Attention to this important step ensures well-crafted policies that address current needs but also consider future technologies that may impact student data privacy. While proactive protection may be an amorphous concept, FPF has sought to make it an actionable step by providing suggestions for incorporating this step into written policies. The framework also provides a list of questions that policymakers can use to guide this process.

VI. PROACTIVE PROTECTION OF STUDENT DATA PRIVACY

1) Educational agencies and institutions and their third parties should seek to eliminate student privacy concerns before they arise through ongoing convenings with diverse stakeholders where privacy, equity, and ethical issues are explored in-depth.

1) Education agencies and institutions and their third parties should seek to eliminate student data privacy concerns before they arise, by conducting regular convenings with diverse stakeholders to explore privacy and related equity and ethical issues in depth.

In addition to practicing the elements outlined above, education agencies and institutions (or groups hoping to work with them) should seek to eliminate student data privacy concerns before they arise. The most effective way to do this is by convening diverse stakeholders, especially those working directly with students, to explore the potential impacts of new or changed programs or initiatives. States can pass policies encouraging these ongoing summits or even mandating that one of the governance boards or community groups detailed above discuss some of the broad privacy and equity issues that exist.

The first set of questions can spark conversations that may mitigate student privacy risks and improve data governance, equity, and the success of programs and initiatives. Many questions were adapted from Artefact Group's "Tarot Cards of Tech."[182]

Mitigating Harm

- What could a bad actor do with the data or technologies used by your program or initiative?
  - What could predatory or exploitative behavior look like?
- Which data collected by the program or initiative would be embarrassing or harmful to a student if it were available to the public? Is that data necessary? If so, how long does it need to be kept? Could the data be deidentified?
- How could the data collected be used to harm a student or students?
- What harms could occur if a student is part of any of the following marginalized groups and their data is released publicly or used inappropriately?
  - Students who may be racially profiled;
  - Students with invisible disabilities;
  - Students who are LGBTQIA with families that would harm or kick them out if they knew;
  - Students facing abuse at home;
  - Students who are undocumented or whose families are undocumented;
  - Students who are experiencing homelessness;
  - Student activists;
  - Students who may not have access to a computer, a tablet, or a phone;
  - Students who may not have access to the internet or may have metered or slow internet;
- How obvious are the behavioral change strategies that your program or initiative uses? How does any technology used by the program or initiative encourage users to engage, and how does it make it easy to disconnect?
- How does your program or initiative respect people's boundaries and the other parts of their lives?

Perception Issues

- What about the program or initiative would concern the following types of people the most, and how could those concerns be assuaged (if possible)?
  - A parent or adult student who does not trust the government (including education agencies and institutions) when it has access to student data;
  - A parent or adult student who does not trust for-profit companies (especially technology companies) when they have access to student data;
  - A parent or adult student who believes that data-driven programs are based on explicitly or implicitly biased data and are likely to harm them or their children;
  - A parent who believes that it is not a school's role to teach "soft skills" or values to their children;
  - A parent or adult student who is concerned that personalized learning or student success programs limit student potential by putting students on tracks that may not reflect their actual needs or capacity.
- What could cause people to lose trust in the program or initiative?
  - What could make people feel unsafe or exposed?
  - Which mechanisms are in place to gather student, parent, and community feedback?
  - How will you recognize larger patterns in feedback in order to take action?
- What is the creepiest way that a newspaper headline could describe the program or initiative?

- Which personally identifiable data collected by the program or initiative would be valuable to postsecondary institutions or employers regarding decisions about whether to admit or hire students? Who might be outraged or find it creepy if that data were shared for that purpose?
- Who or what disappears if the program or initiative is successful?
    - Who loses their job?
    - Which other products, services, or initiatives are replaced?
    - Which industries, institutions, or policies would be affected?

Many organizations also seek to improve education through data analysis or technology based on algorithms. However, algorithms, like humans, may reflect explicit or implicit biases either in their design, in their underlying data, or in how they are applied. The following set of questions, adapted from the Critical Platform Studies Group and the ACLU of Washington's Algorithmic Equity Toolkit,[183] can help stakeholders pinpoint program or initiative issues that raise privacy or equity concerns.

Accuracy Questions

- How accurate is the system? How often and under what conditions does it make mistakes? Does it have settings to adjust for more-precise predictions?
- What evidence is there, other than the manufacturer's claims, that the system's accuracy has been independently tested?
    - How will the system perform in the local context in which it is deployed?
    - How does the system perform when presented with diverse characteristics such as skin tone, lighting, signal interference, movement, slang used by marginalized communities, different languages, or incomplete information?
- Which policies and procedures are in place when the system makes a mistake?
    - How are users of the system trained to recognize and resolve errors?
    - How do reporting processes publicly disclose errors when they occur?
    - Which mechanisms are in place for auditing outcomes?
    - What is the role of community oversight in monitoring errors and outcomes?
    - What are the penalties for harms resulting from inaccurate assessments?
    - What are the protections for whistleblowers?
- Can the program or initiative demonstrate that
    - The system will not make false or misleading assessments?
    - People using the system are trained to recognize situations in which false results are likely?
    - Robust oversight of the system exists?

Equity Questions

- Where does the system's data come from? Who gathered that data, with what tools, and for what purpose?
    - How has the data been audited to ensure that it does not reflect discriminatory practices such as racial profiling?
    - Will the data be repurposed from the original intention for its collection? If so, how?

- Even if the system works without errors, does it still perpetuate injustice?
  - Do community members provide input into the system's implementation (including where and when the system is used)? Can community members object and have their objections heard?
  - How can students or their parents access and correct system records?
  - What are the intended and allowable uses of the system?
  - Are there oversight mechanisms that ensure the system is used only for the specific purposes claimed? If so, what are they?
  - Are there disciplinary penalties for misuse of the system? If so, what are they?
- Can the program or initiative demonstrate that
  - The system will not replicate historical patterns of bias such as racism and sexism?

CONCLUSION

Effectively using student data can lead to improved outcomes for students, but stakeholders must also acknowledge the associated risks and privacy harms of data use. As states continue to grapple with student data privacy issues, FPF believes that this best practices framework can serve as a model for state and local agencies, as well as postsecondary institutions, that wish to implement responsible student data privacy policies. While few, if any, states, agencies, or institutions may be currently implementing all of the recommended best practices, the examples throughout this report show that the best practices are both practical and achievable. Stakeholders can use this framework as a guide to measure a state's current success, and it can provide a path forward to help states become exemplars of student data privacy. FPF acknowledges that there is no one-size-fits-all approach given the unique needs of each state and local agency and institution. Instead, this framework is designed to help states and institutions advance their student data privacy protection, as a key part of demonstrating how education data and technology can improve students' learning experiences and outcomes.

ENDNOTES

1 *FPF Guide to Protecting Student Data Under SOPIPA: For K-12 School Administrators and Ed Tech Vendors*, Future of Privacy Forum (November 2016), Accessed May 26, 2021, https://fpf.org/wp-content/uploads/2016/11/SOPIPA-Guide_Nov-4-2016.pdf.

2 Dustin Volz, Yahoo says hackers stole data from 500 million accounts in 2014, Reuters, (September 22, 2016), Accessed March 17, 2021, https://www.reuters.com/article/us-yahoo-cyber/yahoo-says-hackers-stole-data-from-500-million-accounts-in-2014-idUSKCN11S16P.

3 Maggie McGrath, Target Data Breach Spilled Info On As Many As 70 Million Customers, Forbes, (January 10, 2014), Accessed March 17, 2021, https://www.forbes.com/sites/maggiemcgrath/2014/01/10/target-data-breach-spilled-info-on-as-many-as-70-million-customers/?sh=5f22a149e795.

4 Dan Swinhoe, The 15 Biggest Data Breaches of the 21st Century, CSO, (January 8, 2021), Accessed March 24, 2021, https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

5 Natasha Singer, InBloom Student Data Repository to Close, The New York Times, (April 21, 2014), Accessed March 17, 2021, https://bits.blogs.nytimes.com/2014/04/21/inbloom-student-data-repository-to-close/.

6 Number of Ed-Tech Tools in Use Has Jumped 90 Percent Since School Closures (7/8/2020), Accessed May 28,2021, https://marketbrief.edweek.org/marketplace-k-12/access-ed-tech-tools-jumped-90-percent-since-school-closures/

7 *Student Privacy State Laws,* Student Privacy Compass, (2021), Accessed May 12, 2021, https://studentprivacycompass.org/state-laws/.

8 In this report, the term "parents" is inclusive of parents, guardians, and other caregivers.

9 *Nothing to Hide: Tools for Talking (and Listening) About Data Privacy for Integrated Data Systems*, Actionable Intelligence for Social Policy and Future of Privacy Forum (October 2018) at 14, Accessed May 12, 2021, https://fpf.org/wp-content/uploads/2018/09/FPF-AISP_Nothing-to-Hide.pdf.

10 *Nothing to Hide: Tools for Talking (and Listening) About Data Privacy for Integrated Data Systems*, Actionable Intelligence for Social Policy and Future of Privacy Forum (October 2018) at 14, Accessed May 12, 2021, https://fpf.org/wp-content/uploads/2018/09/FPF-AISP_Nothing-to-Hide.pdf.

11 As published in Rob Kitchin (complete citation), who compiled it from Solove. https://www.researchgate.net/publication/293755608_Getting_smarter_about_smart_cities_Improving_data_privacy_and_data_security https://www.slideshare.net/robkitchin/privacy-maynooth

12 Nothing to Hide: Tools for Talking (and Listening) About Data Privacy for Integrated Data Systems, Actionable Intelligence for Social Policy and Future of Privacy Forum (October 2018) at 14-15, Accessed May 12, 2021, https://fpf.org/wp-content/uploads/2018/09/FPF-AISP_Nothing-to-Hide.pdf.

13 Anisha Reddy & Amelia Vance, Student Health Information During the COVID-19 Pandemic, Future of Privacy Forum, (March 20, 2020), Accessed June 14, 2021, https://studentprivacycompass.org/covid-19faqs/#Q5.

14 Casey Waughn, Rethinking Video Mandates In Online Classrooms: Privacy and Equity Considerations and Alternative Engagement Methods, Future of Privacy Forum, (December 2, 2020), Accessed June 14, 2021, https://studentprivacycompass.org/videomandates/.

15 Jason P Nance., Student Surveillance, *Racial Inequalities, and Implicit Racial Bias* (August 27, 2016). 66 Emory Law Journal 765 (2017), University of Florida Levin College of Law Research Paper No. 16-30, Available at SSRN: https://ssrn.com/abstract=2830885.

16 Nothing to Hide: Tools for Talking (and Listening) About Data Privacy for Integrated Data Systems, Actionable Intelligence for Social Policy and Future of Privacy Forum (October 2018) at 15, Accessed May 12, 2021, https://fpf.org/wp-content/uploads/2018/09/FPF-AISP_Nothing-to-Hide.pdf.

17 Eligible students under FERPA refer to students over the age of 17 or who are attending a postsecondary institution at any age. For more information, see the Family Educational Rights and Privacy Act Regulations, 34 CFR §99.3.

18 *Protection of Pupil Rights Amendment (PPRA) General Guidance*, U.S. Department of Education (November 2020), Accessed May 12, 2021, https://studentprivacy.ed.gov/sites/default/files/resource_document/file/20-0379.PPRA_508_0.pdf.

19

20

21 S.B. 820, 86th Leg., Reg. Sess. (Tex. 2019).

22 HB 1030, 2015 Gen. Assemb., 2015-2016 Sess. (N.C. 2016) (PII), H.B. 632, 2015-2016 Gen. Assemb., 2016 Sess. (N.C. 2016) (PII), S.B. 321, 131st Gen. Assemb., Reg. Sess. (Ohio 2016) (student records), S.B. 2295, 65th Leg., Reg. Sess. (N.D. 2017) (research records and PII), and H.B. 1664, 2017 Gen. Assemb., 2017 Sess. (Va. 2017) (student records).

23 Ky. Rev. Stat. Ann. § 61.931 (2015).

24 Md. Code. Ann., State Government, §10-13A-01.

25 Rick Ganley and Michael Brindley, *New State Law Complicates Classroom Recording for N.H. School Districts,* NHPR (November 11, 2015), Accessed April 14, 2021, https://www.nhpr.org/post/new-state-law-complicates-classroom-recording-nh-school-districts#stream/0.

26 Amelia Vance and Casey Waughn, *Student Privacy's History of Unintended Consequences,* 44 Seton Hall Legis. J. 515, 542 (2019).

27 *Student Privacy Communications Toolkit: For Schools & Districts*, Student Privacy Compass (January 12, 2021), Accessed April 5, 2021, https://studentprivacycompass.org/resource/student-privacy-communications-toolkit-for-schools-districts/.

28 Education Counsel LLC, *Key Elements for Strengthening State Laws and Policies Pertaining to Student Data Use, Privacy and Security Guidance for State Policymakers*, Appendix A: "State Legislation/Policy Checklist for Student Data Use, Privacy, and Security Laws," p.1-4, (March 2014), https://educationcounsel.com/?publication=key-elements-for-strengthening-state-laws-and-policies-pertaining-to-student-data-use-privacy-and-security-guidance-for-state-policymakers.

29 Foundation for Excellence in Education, *Building A Trusted Environment: A Snapshot of State Laws on Student Data Use, Privacy and Security,* p.7, (May 2015), https://drive.google.com/file/d/1lQfRn9Nlj8-iTMCpOuGGMKuRbNBGOYXD/view?usp=sharing.

30 U.S. Dep't Of Health, Educ., & Welfare, *Records, Computers, and The Rights of Citizens* (1973), Accessed on May 26, 2021, https://www.justice.gov/opcl/docs/rec-com-rights.pdf.

31 Hugo Teufel III, *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security*, Privacy Policy Guidance Memorandum, (December 2008), Accessed May 12, 2021, https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf.

32 *Student Privacy State Laws,* Student Privacy Compass, (2021), Accessed May 12, 2021, https://studentprivacycompass.org/state-laws/.

33 Omer Tene and Jules Polonetsky, A Theory of Creepy: Technology, Privacy and Shifting Social Norms, 16 Yale Journal of Law & Technology, 59 (2013), https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1098&context=yjolt.

34 In this report, the term "parents" is inclusive of parents, guardians, and other caregivers.

35 Neb. Rev. Stat. § 79-2,104 (2019)

36 Corinne Lestch, *Are Student Privacy Laws Hurting Students?*, Ed Scoop (March 2, 2015), https://edscoop.com/are-student-privacy-laws-hurting-students.

37 Louisiana House Education Committee Meeting, supra note 133 (containing testimony from Rep. Schroeder and discussion by AmeliaVance regarding opt-in consent found in original act).

38 https://www.catchon.com/wp-content/uploads/california-student-data-privacy-and-security-highlights.pdf

39 Amelia Vance, Policymaking on Education Data Privacy: Lessons Learned, 2 Education Leaders Report 2, (Apr. 2016), www.nasbe.org/wp-content/uploads/Vance_Lessons-Learned-Final.pdf, at 11.

40 https://nasbe.nyc3.digitaloceanspaces.com/2020/01/Policymaking-on-Education-Data-Privacy_Lessons-Learned.pdf

41 Nothing to Hide: Tools for Talking (and Listening) About Data Privacy for Integrated Data Systems, Actionable Intelligence for Social Policy and Future of Privacy Forum (October 2018) at 14, Accessed May 12, 2021, https://fpf.org/wp-content/uploads/2018/09/FPF-AISP_Nothing-to-Hide.pdf.

42 Amelia Vance, West Virginia's Steady Course on Student Data Privacy, NASBE (February 2016), http://www.nasbe.org/state-innovation/west-virginias-steady-course-onstudent-data-privacy/.

43 Data Quality Campaign, *Student Data Privacy Legislation: A Summary of 2016 State Legislation*, p.6 (September 2016) (citing H.B. 358, 2016 Leg., Gen. Sess. (Utah 2016)), https://drive.google.com/file/d/1Ft6t-TQUBVWEKQW3KVK45saGSYWR3C7B/view.

44 Nate Robson, *State Education Board Votes to Allow Data Release*, Oklahoma Watch (August 31, 2015), Accessed May 31, 2015, https://oklahomawatch.org/2015/08/31/state-education-board-votes-to-allow-data-release/.

45 Amelia Vance, *Policymaking on Education Data Privacy: Lessons Learned,* National Association of State Boards of Education, Education Leaders Report (April 2016), Accessed May 12, 2021, https://nasbe.nyc3.digitaloceanspaces.com/2020/01/Policymaking-on-Education-Data-Privacy_Lessons-Learned.pdf.

46 Vance and Waughn, *supra* note 22, at 542.

47 Vance and Waughn, citing the 2018 committee hearing for PA 17-200. Transcripts from the Joint Standing Committee Public Hearing(s) and/or Senate and House of Representatives Proceedings, Pub. Act No. 16-189, H.B. 7207, Connecticut State Library (2018).

48 H.B. 245, 2019 Leg., Reg. Sess. (Md. 2019).

49 https://le.utah.gov/~2015/bills/static/HB0068.html#53a-1-710

50 N.Y. Educ. Law § 2-D.

51 https://leg1.state.va.us/cgi-bin/legp504.exe?151+ful+CHAP0561

52 http://www.wvlegislature.gov/legisdocs/code/18/WVC%2018%20%20-%20%202%20%20-%20%20%205%20H.htm

53 https://cdt.org/insights/chief-privacy-officers-who-they-are-and-why-education-leaders-need-them/

54 Id.

55 National Center for Education Statistics Institute on Education Sciences, *P-20W+ Data Governance: Tips from the States*, Best Practices Brief, (February 2017), Accessed May 12, 2021, https://slds.ed.gov/services/PDCService.svc/GetPDCDocumentFile?fileId=25962.

56 Utah Code § 53E-9-302(4) (2020).

57 N.Y. Educ. Law § 2-D.

58 N.Y. Educ. Law § 2-D.

59 https://www.congress.gov/bill/114th-congress/house-bill/1831/text

60 Utah Code § 53E-9-302(5) (2020).

61 http://www.wvlegislature.gov/Bill_Status/bills_text.cfm?billdoc=hb4316%20SUB%20ENR.htm&yr=2014&sesstype=RS&billtype=B&houseorig=H&i=4316

62 https://thehill.com/opinion/cybersecurity/363095-securing-student-data-is-a-challenge-that-requires-cash

63 https://www.catchon.com/wp-content/uploads/florida-student-data-privacy-and-security-highlights.pdf

64 https://casetext.com/regulation/alaska-administrative-code/title-4-education-and-early-development/chapter-52-education-for-children-with-disabilities-and-gifted-children/article-2-program-administration-children-with-disabilities/section-4-aac-52765-protection-of-records

65 Jasmine Park et al., *Student Privacy Communications Toolkit: For Schools and Districts*, Student Privacy Compass, (2021), Accessed May 12, 2021, https://studentprivacycompass.org/resource/student-privacy-communications-toolkit-for-schools-districts/.

66 N.J. Rev. Stat §18A:36-19 (2013).

67 https://legislature.idaho.gov/wp-content/uploads/sessioninfo/2014/legislation/S1372.pdf

68 https://www.catchon.com/wp-content/uploads/new-york-student-data-privacy-and-security-highlights.pdf

69 Amelia Vance, Policymaking on Education Data Privacy: Lessons Learned, Education Leaders Report, National State Boards of Education, (2016) https://nasbe.nyc3.digitaloceanspaces.com/2020/01/Policymaking-on-Education-Data-Privacy_Lessons-Learned.pdf (citing W. Va. Code § 18B-1D-10, Neb. Rev. Stat. § 79-2,104).

70 *Id.*

71 H.B. 1989 2013 Leg., Reg. Sess. (Okla. 2013).

72 *Amelia Vance, West Virginia's Steady Course on Student Data Privacy, National Association of State Boards of Education, p.2 (February 2016).*

73 Forum Guide to Data Governance, National Forum on Education Statistics (June 2020), Accessed June 10, 2021, https://nces.ed.gov/pubs2020/NFES2020083.pdf.

74 Maryland General Assembly, HB 1122 (2020), State Government - Protection of Personally Identifiable Information - Public Institutions of Higher Education, enacted May 8, 2020, codified at Md. Code Ann. State Government § 10-13A-01 to take effect October 1, 2024.

75 https://www.catchon.com/wp-content/uploads/illinois-student-data-privacy-and-security-highlights.pdf

76 https://ib5uamau5i20f0e91hn3ue14-wpengine.netdna-ssl.com/wp-content/uploads/2015/08/Building-A-Trusted-Environment-A-Snapshot-of-State-Laws-on-Student-Data-Use-Privacy-and-Security.pdf

77 http://kslegislature.org/li_2014/b2013_14/statute/072_000_0000_chapter/072_062_0000_article/072_062_0017_section/072_062_0017_k/

78 8 NY C.R.R. Part 121 (2020).

79 EducationCounsel, *Key Elements for Strengthening State Laws and Policies Pertaining to Student Data Use, Privacy, and Security: Guidance for State Policymakers*, Guidance on State Student Privacy and Security Policies, (March 2014), Accessed May 12, 2021, https://ib5uamau5i20f0e91hn3ue14-wpengine.netdna-ssl.com/wp-content/uploads/2015/06/EducationCounsel%20Guidance%20on%20State%20Student%20Privacy%20and%20Security%20Policies%20-%204838-6763-1641%20v%202.pdf; National Council of State Education Attorneys, *State Education Agency Data Sharing and the Family Education Rights and Privacy Act,* (June 2020), Accessed May 12, 2021, https://nasbe.nyc3.digitaloceanspaces.com/2020/11/NCOSEA-FERPA_Final-Paper-2020.pdf.

80 Jasmine Park et al., *Student Privacy Communications Toolkit: For Schools and Districts*, Student Privacy Compass, (2021), Accessed May 12, 2021, https://studentprivacycompass.org/resource/student-privacy-communications-toolkit-for-schools-districts/.

81 Education Counsel LLC, *Key Elements for Strengthening State Laws and Policies Pertaining to Student Data Use, Privacy and Security Guidance for State Policymakers*, p.7, (March 2014), https://educationcounsel.com/?publication=key-elements-for-strengthening-state-laws-and-policies-pertaining-to-student-data-use-privacy-and-security-guidance-for-state-policymakers.

82 Appendix A: The Consumer Privacy Bill of Rights, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, The White House (February 2012), https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf.

83 Legitimate Interests, Guide to the General Data Protection Regulation (GDPR), Information Commissioner's Office (ICO), Accessed June 9, 2021, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/.

84 H.B. 1989 2013 Leg., Reg. Sess. (Okla. 2013).

85 Tenn. Code § 49-1-703 (2019).

86 H.B. 1989 2013 Leg., Reg. Sess. (Okla. 2013).

87 Tenn. Code § 49-1-703 (2019).

88 Colorado Department of Education, *SchoolView,* DataCenter, (2021), Accessed on May 12, 2021, https://edx.cde.state.co.us/SchoolView/DataCenter/reports.jspx?_adf_ctrl-state=pac20phbp_4&_afrLoop=9029575540655965&_afrWindowMode=0&_adf.ctrl-state=phv6bj3c9_4.

89 Id.

90 National Center for Education Statistics Institute on Education Sciences, *P-20W+ Data Governance: Tips from the States*, Best Practices Brief, (February 2017), Accessed May 12, 2021, https://slds.ed.gov/services/PDCService.svc/GetPDCDocumentFile?fileId=25962.

91 Washington State Education Research & Data Center, (2019), Accessed May 12, 2021, https://erdc.wa.gov/.

92 National Center for Education Statistics Institute on Education Sciences, *P-20W+ Data Governance: Tips from the States*, Best Practices Brief, (February 2017), Accessed May 12, 2021, https://slds.ed.gov/services/PDCService.svc/GetPDCDocumentFile?fileId=25962.

93 Center for Educational Performance and Information, *How Your Data Are Used*, (2021), Accessed May 12, 2021, https://www.michigan.gov/cepi/0,4546,7-113--252460--,00.html.

94 Center for Educational Performance and Information, *How CEPI Protects Education Data*, (2021), Accessed May 12, 2021, https://www.michigan.gov/cepi/0,4546,7-113-985-336886--,00.html.

95 https://mgaleg.maryland.gov/2010rs/chapters_noln/ch_190_sb0275e.pdf

96 State Longitudinal Data Systems, *New York*, State Profile, (2019), Accessed May 12, 2021, http://slds.rhaskell.org/state-profiles/new-york.

97 State Longitudinal Data Systems, *Ohio*, State Profile, (2019), Accessed May 12, 2021, http://slds.rhaskell.org/state-profiles/ohio.

98 City of Seattle Open Data Risk Assessment, Future of Privacy Forum (January 2018), Accessed June 9, 2021, https://fpf.org/wp-content/uploads/2018/01/FPF-Open-Data-Risk-Assessment-for-City-of-Seattle.pdf.

99 Data Governance, Colorado Department of Education, (2019), Accessed May 12, 2021, https://www.cde.state.co.us/cdereval/datagovernance.

100 Student Data Principles, Data Quality Campaign and the Consortium for School Networking (2014), Accessed June 16, 2021, https://studentdataprinciples.org/the-principles/.

101 EducationCounsel, *Key Elements for Strengthening State Laws and Policies Pertaining to Student Data Use, Privacy, and Security: Guidance for State Policymakers*, (March 2014), Accessed June 16, 2021, https://educationcounsel.com/?publication=key-elements-for-strengthening-state-laws-and-policies-pertaining-to-student-data-use-privacy-and-security-guidance-for-state-policymakers (citing S.B. 275, 2010 Leg., Reg. Sess. (Md. 2010)).

102 Forum Guide to Data Governance, National Forum on Education Statistics (June 2020), Accessed June 8, 2021, https://nces.ed.gov/pubs2020/NFES2020083.pdf.

103 EducationCounsel, Key Elements for Strengthening State Laws and Policies Pertaining to Student Data Use, Privacy, and Security: Guidance for State Policymakers, Guidance on State Student Privacy and Security Policies, p. 7 (March 2014), Accessed June 16, 2021,https://educationcounsel.com/?publication=key-elements-for-strengthening-state-laws-and-policies-pertaining-to-student-data-use-privacy-and-security-guidance-for-state-policymakers.

104 https://slate.com/technology/2017/01/how-to-protect-students-personal-data.html

105 Eastern Michigan University, PII- Personally Identifiable Information-Training and Fraud Prevention [PowerPoint Slides], Accessed May 12, 2021, https://www.emich.edu/privacy/documents/campus-pii-training-summary-final.pdf.

106 H.B. 1348, 66th Leg. Assemb., 2019 Sess. (N.D. 2019).

107 Data Quality Campaign, *Education Data Legislative Review: 2017 State Activity*, p.5 (September 2017), https://drive.google.com/file/d/1nDbVwYbVfpTPkbTvoynAYujr24pMW_63/view?usp=sharing.

108 *Student Privacy State Laws,* Student Privacy Compass, (2021), Accessed May 12, 2021, https://studentprivacycompass.org/state-laws/.

109 H.B. 363, 2021 Leg., Reg. Sess. (Tex. 2021).

110 Texas Ed. Code § 32.153

111 Texas Ed. Code § 32.152

112 A.B. 1584, 2013-2014 Leg., Reg. Sess. (Cal. 2014) (added §49073.1 to Cal. Educ. Code).

113 Kelsey Finch, *De-Identification*, Future of Privacy Forum, (April 2021), Accessed May 12, 2021, https://fpf.org/issue/deid/.

114 The Department of Homeland Security, *The Fair Information Practice Principles*, Internal Directives, Strategy and Doctrinal Products, (August 2015), Accessed May 12, 2021, https://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2008-01-fair-information-practice-principles; Ann Cavoulian, *Privacy as the Default Setting*, Privacy by Design: The Seven Foundational Principles, (January 2011), Accessed May 12, 2021, https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf.

115 *SLDS Webinar: Use of Research Analytics in SLDS*, SLDS Grant Program, (2015), Accessed May 25, 2021, https://slds.ed.gov/#communities/pdc/documents/7729.

116 Privacy Technical Assistance Center, *Best Practices for Data Destruction*, (May 2014), Accessed May 12, 2021, https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Best%20Practices%20for%20Data%20Destruction%20%282019-3-26%29.pdf.

117 Kan. Stat. § 72-6217(2014).

118 Utah State Board of Education, *UTAH RAMP: Utah Education Records Retention Schedule* (May, 11 2020), Accessed May 27, 2021, https://schools.utah.gov/file/778b33ae-2617-4793-b2d1-d9a0b46070dc.

119 https://www.wsj.com/articles/one-parent-is-on-a-mission-to-protect-children-from-digital-mistakes-11562762000

120 Todd Feathers, *Major Universities Are Using Race as a "High Impact Predictor" of Student Success*, The Markup, (March 2, 2021), Accessed May 21, 2021, https://themarkup.org/news/2021/03/02/major-universities-are-using-race-as-a-high-impact-predictor-of-student-success.

121 EdTrust, *Joint Memo on Advancing Educational Equity Through the Biden-Harris Administration*, EdTrust, (Dec. 2, 2020), Accessed May 21, 2021, https://edtrust.org/press-release/joint-memo-on-advancing-educational-equity-through-the-biden-harris-administration/.

122 Emily Boudreau, *Measuring Implicit Bias in Schools*, Harvard Graduate School of Education, (August 1, 2020), Accessed May 21,2021, https://www.gse.harvard.edu/news/uk/20/08/measuring-implicit-bias-schools; Tasminda K. Dhaliwal et. al., *Educator bias is associated with racial disparities in student achievement and discipline*, The Brookings Inst., (July 20, 2020), Accessed May 21, 2021, https://www.brookings.edu/blog/brown-center-chalkboard/2020/07/20/educator-bias-is-associated-with-racial-disparities-in-student-achievement-and-discipline/.

123 Amelia Vance and Sarah Williamson, Law Enforcement Access to Student Records: A Guide for School Administrators & EdTech Service Providers, (September 2017), Accessed May 21, 2021, https://studentprivacycompass.org/law-enforcement-access-to-student-records/.

124 Conn. Gen. Stat. § 10-234bb; Idaho Code § 33-133; Kan. Stat. Ann. § 72-6314(c).

125 Kan. Stat. Ann. § 72-6314(c); Mo. Ann. Stat. § 161.096.

126 *See Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices*, U.S. Department of Education (February 2014), Accessed May 25, 2021, https://studentprivacy.ed.gov/resources/protecting-student-privacy-while-using-online-educational-services-requirements-and-best; *Student Privacy Communications Toolkit: For Schools & Districts*, Student Privacy Compass (January 12, 2021), Accessed April 5, 2021, https://studentprivacycompass.org/resource/student-privacy-communications-toolkit-for-schools-districts/.

127 The Department of Homeland Security, *The Fair Information Practice Principles*, Internal Directives, Strategy and Doctrinal Products, (August 2015), Accessed May 12, 2021, https://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2008-01-fair-information-practice-principles

128 8 NY C.R.R. Part 121, §121.13 (2020).

129 8 NY C.R.R. Part 121, §121.6 (2020).

130 Common Sense Media, *Assessing State Laws on Student Privacy in 2014 and Beyond: A School Privacy Zone Update from Common Sense Kids Action* (2015), p. 7, https://www.commonsensemedia.org/sites/default/files/uploads/kids_action/csm-privacy-report-interactive-070215-proof-3.pdf.

131 Celeste Alexander and Corey Chatis, *Texas's Education Research Centers*, SLDS Spotlight, (May 2017), Accessed May 12, 2021, https://slds.ed.gov/services/PDCService.svc/GetPDCDocumentFile?fileId=26865.

132 Julie Eklund et al., *Research Request Processes; Lessons Learned and Outcomes*, SLDS Grant Program, (November 2018), Accessed May 12, 2021, https://slds.ed.gov/#communities/pdc/documents/17610.

133 Marie Bienkowski, *Implications of Privacy Concerns for Using Student Data for Research: Panel Summary*, National Academy of Education (2017), Accessed June 9, 2021, https://naeducation.org/wp-content/uploads/2017/05/Bienkowski-FINAL.pdf.

134 Marie Bienkowski, *Implications of Privacy Concerns for Using Student Data for Research: Panel Summary*, National Academy of Education (2017), Accessed June 9, 2021, https://naeducation.org/wp-content/uploads/2017/05/Bienkowski-FINAL.pdf.

135 Marie Bienkowski, *Implications of Privacy Concerns for Using Student Data for Research: Panel Summary*, National Academy of Education (2017), Accessed June 9, 2021, https://naeducation.org/wp-content/uploads/2017/05/Bienkowski-FINAL.pdf.

136 https://naeducation.org/wp-content/uploads/2017/05/Bienkowski-FINAL.pdf

137 Jules Polonetsky, Omer Tene, & Kelsey Finch, *Shades of Grey: Seeing the Full Spectrum of Practical Data De-identification*, 56 Santa Clara L. Rev. 593 (2016), Accessed May 21, 2021, https://digitalcommons.law.scu.edu/lawreview/vol56/iss3/3.; City of Seattle Open Data Risk Assessment, Future of Privacy Forum (January 2018), Accessed June 9, 2021, https://fpf.org/wp-content/uploads/2018/01/FPF-Open-Data-Risk-Assessment-for-City-of-Seattle.pdf.

138 Jules Polonetsky, Omer Tene, & Kelsey Finch, *Shades of Grey: Seeing the Full Spectrum of Practical Data De-identification*, 56 Santa Clara L. Rev. 593 (2016), Accessed May 21, 2021, https://digitalcommons.law.scu.edu/lawreview/vol56/iss3/3.

139 Eastern Michigan University, PII- Personally Identifiable Information-Training and Fraud Prevention [PowerPoint Slides], Accessed May 12, 2021, https://www.emich.edu/privacy/documents/campus-pii-training-summary-final.pdf.

140 H.B. 1348, 66th Leg. Assemb., 2019 Sess. (N.D. 2019).

141 https://boardofed.idaho.gov/resources/model-student-data-privacy-and-security-policy/

142 Student Data Privacy: A Toolkit for Connecticut School Districts, Connecticut Commission for Educational Technology (July 10, 2017), Accessed May 31, 2021, https://portal.ct.gov/-/media/DAS/CTEdTech/publications/2017/StudentDataPrivacyToolkit_V1.pdf.

143 201 Mass. Code Reg. 17.00 (2017).

144 Sandra G. Mayson, Bias In, Bias Out, The Yale Law Journal (2019), 2221-2300, https://www.yalelawjournal.org/pdf/Mayson_p5g2tz2m.pdf.

145 City of Seattle Open Data Risk Assessment, Future of Privacy Forum (January 2018), Accessed June 9, 2021, https://fpf.org/wp-content/uploads/2018/01/FPF-Open-Data-Risk-Assessment-for-City-of-Seattle.pdf.

146 Elisa Jillson, Aiming for Truth, Fairness, and Equity in Your Company's Use of AI, Business Blog, (April 19, 2021), Accessed on May 12, 2021, https://www.ftc.gov/news-events/blogs/business-blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai.

147 *Privacy Impact Assessments,* Department of Homeland Security (November 25, 2020), Accessed May 27, 2021, https://www.dhs.gov/privacy-impact-assessments

148 *UW Personal Data Processing Task Force Charge Letter*, University of Washington Privacy Office (November 3, 2020), Accessed May 27, 2021, https://privacy.uw.edu/about-us/governance/pdp-charge-letter/.

149 *Privacy Assessments*, University of Washington Privacy Office, Accessed May 27, 2021, https://privacy.uw.edu/design/privacy-assessments/.

150 West Virginia Department of Education, Data Privacy, Accessed May 2021, https://wvde.state.wv.us/zoomwv/data-privacy.html.

151 West Virginia Department of Education, *Data Access & Management Guidance*, (2014), Accessed May 2021, http://static.k12.wv.us/tt/2014/datamanagement_guidance%20FINAL%201-21-14.pdf.

152 West Virginia Department of Education, *Protecting the Privacy and Confidentiality of Student Data, (October 2014), Accessed May 2021,* http://static.k12.wv.us/zoomwv/protecting-the-privacy-and-confidentiality-of-student-data.pdf

153 Colorado Department of Education, *Data Privacy and Security,* (April 13, 2020), Accessed May 12, 2021, https://www.cde.state.co.us/dataprivacyandsecurity.

154 https://fpf.org/wp-content/uploads/2018/01/FPF-Open-Data-Risk-Assessment-for-City-of-Seattle.pdf

155 collection, use, sharing, retention, and storage of student information; Ann Cavoulian, Visibility and transparency - Keep It Open, Privacy by Design: The Seven Foundational Principles, (January 2011), Accessed May 12, 2021, https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf.

156 Utah State Board of Education, USBE Data Gateway, (2021), Accessed May 12, 2021, https://datagateway.schools.utah.gov/DataDictionary/Home/Agreement/7?leaId=99.

157 Jasmine Park et al., Student Privacy Communications Toolkit: For Schools and Districts, Student Privacy Compass, (2021), Accessed May 12, 2021, https://studentprivacycompass.org/resource/student-privacy-communications-toolkit-for-schools-districts/.

158 Cory Chatis and Kathy Gosa, Communicating the Value of Data Governance, SLDS Issue Brief, (2017), Accessed May 12, 2021, https://slds.ed.gov/services/PDCService.svc/GetPDCDocumentFile?fileId=28771.

159 Scott LaFee, Transparency, The American Association of School Administrators, (2019), Accessed May 12, 2021, https://www.aasa.org/schooladministratorarticle.aspx?id=3532.

160 Board of Education, Metro Nashville Public Schools, (2021), Accessed May 12, 2021, https://www.mnps.org/board-of-education.

161 P-20 Council, Proposed Minutes, (March 25th, 2021), Accessed May 12, 2021, https://www.michigan.gov/documents/cepi/P20-Minutes_501846_7.pdf.

162 Id.

163 State of Connecticut, LearnPlatform, (2021), Accessed May 12, 2021, https://connecticut.learnplatform.com/.

164 https://fpf.org/wp-content/uploads/2018/09/FPF-AISP_Nothing-to-Hide.pdf

165 Ann Cavoukian, *Visibility and transparency - Keep It Open*, Privacy by Design: The Seven Foundational Principles, (January 2011), Accessed May 12, 2021, https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf.

166 Sharon Slade and Alan Tait, *Global Guidelines: Ethics in Learning Analytics*, International Council for Open and Distance Education, (March 2019), Accessed May 12, 2021, https://static1.squarespace.com/static/5b99664675f9eea7a3ecee82/t/5ca37c2a24a694a94e0e515c/1554218087775/Global+guidelines+for+Ethics+in+Learning+Analytics+Web+ready+March+2019.pdf

167 Sharon Slade and Alan Tait, *Global Guidelines: Ethics in Learning Analytics*, International Council for Open and Distance Education, (March 2019), Accessed May 12, 2021, https://static1.squarespace.com/static/5b99664675f9eea7a3ecee82/t/5ca37c2a24a694a94e0e515c/1554218087775/Global+guidelines+for+Ethics+in+Learning+Analytics+Web+ready+March+2019.pdf

168 IT@OSU, *Privacy at Ohio State*, Policies and Standards, (2021), Accessed May 12, 2021, https://it.osu.edu/privacy.

169 IT@OSU, *2020 Privacy Program Year in Review,* (2021), Accessed May 12, 2021, https://it.osu.edu/2020-privacy-program-year-review.

170 Matthew Gault, Facial Recognition Software Regularly Misgenders Trans People, VICE, (February 19, 2019), Accessed June 9, 2021, https://www.vice.com/en/article/7xnwed/facial-recognition-software-regularly-misgenders-trans-people.

171 Surveillance Self-Defence, *Privacy for Students*, (March 2, 2020), Accessed May 12, 2021, https://ssd.eff.org/en/module/privacy-students.

172 Id.

173 US Department of Education, *Family Education Rights and Privacy Act (FERPA)*, (December 2020), Accessed May 12, 2021, https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html.

174 SchoolHouse Connection, 6 Things to Know About Privacy, FERPA, and Homelessness, SchoolHouse Connection, (May 5, 2020), Accessed Jun 14, 2021, https://schoolhouseconnection.org/6-things-to-know-about-ferpa/.

175 US Department of Education, *Ferpa General Guidance for Parents*, (June 2015), Accessed May 12, 2021, https://www2.ed.gov/policy/gen/guid/fpco/ferpa/parents.html.

176 Data Quality Campaign, *Creating a Longitudinal Data System: Using Data to Improve Student Achievement,* (2006), https://dataqualitycampaign.org/wp-content/uploads/2016/03/109_Publications-Creating_Longitudinal_Data_System.pdf.

177 Amelia Vance, *Policy Making on Data Privacy: Lessons Learned,* Education Leaders Report, (April 2016), Accessed on May 12, 2021, https://nasbe.nyc3.digitaloceanspaces.com/2020/01/Policymaking-on-Education-Data-Privacy_Lessons-Learned.pdf.

178 Id.

179 This spectrum is an edited version of FPF's use of the spectrum in Future of Privacy Forum, *Nothing to Hide: Tools for Talking (and Listening) About Data Privacy for Integrated Systems*, (2018), Accessed June 29, 2021, https://fpf.org/wp-content/uploads/2018/09/FPF-AISP_Nothing-to-Hide.pdf. The original spectrum is at International Association for Public Participation, *iap2 public participation spectrum,* (n.d.), https://www2.fgcu.edu/Provost/files/IAP_Public_Participation_Spectrum.pdf.

180 https://dataqualitycampaign.org/resource/metro-nashville-students-define-goals-see-success-data/

181 https://dataqualitycampaign.org/resource/empowering-parents-nashville-data-chats/

182 http://tarotcardsoftech.artefactgroup.com/

183 https://www.aclu-wa.org/AEKit


FUTURE OF
PRIVACY
FORUM