EDUCATION COMMISSION OF THE STATES

SPECIAL REPORT
NOV 2022

State Strategies to Protect Student Data Privacy

Claus von Zastrow and Zeke Perez Jr.

Advances in state education data systems are helping schools understand and meet the needs of learners from early education through college and the workforce. Sophisticated systems for collecting, analyzing, sharing and reporting on student data can empower policymakers, educators, families and students to make more informed decisions about education.

However, when students' private information becomes public, families and students can lose that power, with possibly ruinous consequences for their reputations and life prospects. This Special Report presents three brief case studies of state agencies that have developed effective structures and processes to protect the privacy of students' data without compromising data systems' value as engines of improvement.

Each state has adhered to key principles for protecting student data privacy. In an Education Commission of the States Thinkers Meeting summarized in this Policy Guide, leading experts and practitioners described five key principles for data privacy: a coherent vision for data privacy, coherent legislation, effective data governance structures, training and support for those charged with safeguarding student data, and transparency about their privacy efforts.

The case studies below demonstrate how state leaders can use these principles as guardrails for protecting students' privacy while maximizing the value of student

Key Principles for Data Privacy (From Lessons in Data Privacy for Education Leaders)

- **A Coherent Vision.** A coherent and sustaining vision for education data privacy articulates the benefits of data systems to individuals and society.
- **Coherent Laws.** Coherent and well-implemented data privacy laws help leaders enforce that vision.
- **Governance Structures.** Robust governance structures create clear roles, responsibilities and processes for collecting education data, reporting on it, promoting its quality and maintaining its security.
- **Training and Support.** Training helps stakeholders understand and carry out their respective roles in forming a cohesive system for protecting student privacy.
- **Transparency.** Transparency promotes public trust in data systems by helping students and their families understand and act on their rights to personal data.

data. Two of the case studies — those featuring **Colorado** and **Utah** — examine student privacy policies and practices in the state education agency. The third, which features **Kentucky**, describes privacy policies that operate both in a statewide longitudinal data system and in the agencies that make up that system. Despite differences in data system structure, the principles provide an effective frame for understanding student data privacy.

Building Public Trust in Colorado

As public concern about student data privacy intensified across the country in 2013 and 2014, a large school district in Colorado found itself at the center of the controversy. Jefferson County Public Schools faced mounting criticism from parents and others for its role as one of nine jurisdictions across the country that was piloting InBloom, an initiative that aimed to improve schools by creating a central, open-source platform for data sharing, learning apps and curricula.

A growing chorus of critics maintained that InBloom could expose sensitive student data to private companies or hackers, ultimately prompting the Colorado district to withdraw from the initiative. Soon thereafter, InBloom closed its doors.

According to Marcia Bohannon, chief information officer at Colorado's Department of Education, "InBloom and new technologies like cloud data storage made [Colorado state school] board members worry about risks to student privacy." Privacy became a priority for the state board as well as for state legislators, who began designing legislation to protect students' personal information.

The agency's data privacy practices had already been sound, Bohannon said, but growing privacy concerns and new legislation inspired measures to build Coloradans' trust in student data systems. "We were well regarded outside of Colorado," she noted, "but we needed to win the trust of people in the state." To do so, agency leaders have worked to formalize and document their practices while giving districts training and resources to help them strengthen privacy protections at the local level.

Vision: Supporting Colorado's Youth

Colorado underpins its student data privacy efforts with a public statement defining how it uses data: "The use of data helps guide parents, teachers, schools, districts and state leaders as we work together to improve student

achievement so all children graduate ready for college and career." The department of education pursues that vision while fulfilling a "moral and legal responsibility to protect student privacy and ensure data confidentiality." The agency's vision for why data matters is a useful model for critical data privacy decisions. Unless required by federal or state law, Bohannon said, the agency does not collect data that does not support its vision.

Coherent Laws: Responding to Data Privacy Concerns

Student data privacy laws in Colorado aim to foster public trust in elementary and secondary data systems by promoting transparency and requiring security measures. The state established the foundation for transparency with its initial legislation in 2014. The Student Data Accessibility, Transparency and Accountability Act set a standard of information sharing by mandating publicly available data dictionaries, developing user-friendly resources on the department's data sharing agreements and very clearly delineating detailed components of a data security plan.

The state built on this strong foundation in 2016, passing the Student Data Transparency and Security Act. This new bill refined and added to the existing data privacy definitions and requirements. It required the state to develop a sample student information privacy and protection policy and required all local education providers – which include school districts, Colorado BOCES Association (Boards of Cooperative Educational Services) and charter schools – to adopt such a policy. It also recognizes parents' right to have access to their children's personal data and requires local education providers to adopt a policy allowing parental feedback on providers' data policies.

Colorado Student Data Privacy Laws

H.B. 1294: The Student Data Accessibility, Transparency and Accountability Act requires the state board to publish a publicly available inventory of data elements collected and used in the state data system. It requires the state to develop a comprehensive data security plan, including data access guidelines, privacy and security audits, security breach planning and notification and staff training regarding privacy policies.

H.B. 1423: The Student Data Transparency and Security Act provides new data privacy requirements for the state board, the department of education and local education providers. Notably, local education providers are required to adopt student information privacy and protection policies. The bill also sets guidelines for contract providers' use of students' private information and describes parents' rights over that information.

Colorado's legislative efforts have earned recognition from some of the very organizations that criticized InBloom. The state earned first place in a 2019 student data privacy report card by The Parent Coalition for Student Privacy and the Network for Public Education.

Governance: Making Data Privacy an Organizational Commitment

The Colorado Department of Education's robust governance structure supports implementation of the state's privacy laws by clearly defining how decisions about student data are made, communicated, monitored and enforced. The governance structure also lays out the distinct roles and responsibilities of everyone who makes and abides by those decisions, establishing what Bohannon called a "continuous chain of authority over sensitive data" from the moment it is collected to the time it is reported or destroyed.

The governance structure maintains that chain of authority by assigning a data owner and data coordinator to every data element the department collects. Data owners at the agency help define how to collect, use and report data in ways that ensure accuracy and adhere to privacy requirements. Data coordinators work with data owners to manage data throughout its lifecycle from collection to reporting. Data owners and coordinators bring questions or concerns about data collection and use to governance committees comprising department staff and executive leadership.

According to Bohannon, the agency's governance structure helped it protect sensitive data while responding to complex and urgent data requests from policymakers and education leaders who struggled to address students' needs during the COVID-19 pandemic. The state's system of data owners and coordinators made it easier to communicate what kinds of data were available, what data the agency simply did not collect and what data it could not share. The governance structure also supported orderly decision-making amid a crisis. "Stick with your processes," Bohannon said, "accelerate if necessary, but don't leave out any steps that protect sensitive data. With a good governance structure, you don't have to make too many big decisions on the fly."

Bohannon credits data privacy champions in her agency with helping sustain the organization-wide focus on privacy. For example, Chief Assessment Officer Joyce Zurkowski is a vocal advocate for exacting privacy practices with agency staff who are not directly involved in data management and security. For the

department's governance structure to succeed, Bohannon insisted, "privacy has to be an organization-wide role, not just an information technology role or the job of a single privacy director."

Training and Support: Supporting Districts and Teachers Through Data Privacy Training

In addition to regularly training its own employees, the Colorado Department of Education offers local education providers training, dozens of written model privacy policies, and sample vendor contract language on confidentiality, privacy and security.

All new agency employees must participate in annual training on the fundamentals of information security and privacy, and the agency offers more targeted training for staff who handle private student data. The agency also offers local school districts training and guidance on best practices and compliance with federal and state privacy laws. The agency's data privacy and security webpage features training for teachers developed by the Utah State Board of Education.

When the pandemic shuttered schools, the Colorado Department of Education produced materials to help local educators address the unique privacy challenges that emerged as classrooms moved online. Materials include information on the security of collaboration tools like Zoom or Google Hangouts and best practices for protecting students' privacy during remote learning.

Transparency: Fostering Trust

Faced with new data privacy legislation, leaders at the Colorado Department of Education first set about improving transparency. "You have to be open and transparent about your privacy measures," Bohannon said. "Even the best privacy practices won't have the intended effect if they don't improve public trust."

Before state laws took effect, she noted, staff at her agency followed proper protocols, but the agency did not publicly describe those protocols. In addition, staff responded to legitimate data requests without documenting them, and descriptions of what data the agency collected were difficult or impossible to find on the website.

In addition to posting its policies for protecting students' personal information, the Colorado Department of Education now publishes a searchable data dictionary, which contains descriptions of every data element the agency collects with an indicator of which elements could be used to identify individual students or staff. The agency also publishes an inventory with links to each data sharing agreement it has executed since early 2016, allowing visitors to explore the kinds of data the agency has shared, and with whom.

Bohannon pointed out that simply publishing this information was not enough: "We went through it multiple times until we got it into a format that made sense to people who aren't data experts."

Even if they have the most effective privacy practices, states cannot build trust if they do not communicate with the public about those practices. "You have to talk about what you're doing," Bohannon insisted. "You can't hide it."

Building Capacity in Utah

Utah is widely respected for its education data systems, particularly for its efforts to build strong data governance and elevate data privacy. In particular, the Utah Legislature has focused on testing and growing scalable solutions to data privacy challenges by transforming early explorations into comprehensive and adaptable state policies.

Data leaders in Utah note that flexible data privacy policies help the state adapt to the ever-changing nature of technology, data system infrastructure and data collection. Strong leadership roles and ground-level training also contribute to the longevity and public credibility of the state's data systems.

Vision: Portraying Data Systems as Public Assets

Before addressing student data privacy, the state board of education's main data security and privacy webpage begins with a statement of why data matters: "In this age of data-driven decision making, data is foundational to the success of the process. Whether discussing student achievement, program monitoring, education funding, accountability or any other education-related conversation, data is at the center of the discussion."

The state board grounds its privacy policies in a vision of how data helps Utah, thereby helping state residents see data systems as public assets that require careful management, rather than intrusive government mechanisms that threaten their privacy.

Coherent Laws: Adapting to the State's Unique and Changing Needs

Instead of emulating other states, Utah began its data privacy policy process with careful due diligence to create a law that would meet the state's needs. According to David Sallay, the state board's former chief privacy officer, state leaders tend to start small when tackling a new policy issue: "They understand the potential outcomes and make necessary adjustments before going big."

Utah legislators had concerns about student data privacy, so they started with exploratory legislation in 2015. The bill required and authorized funding for a chief privacy officer within the state board of education and required the board to study options for updating student privacy laws before making recommendations to the Legislature.

In a 2016 interview, Sen. Jacob Anderegg, a student data advocate and primary sponsor of student data privacy bills in the state, described several questions data privacy laws sought to answer: "Number one, what can be collected — what's required, what's optional, and what's prohibited? Number two, how is that information going to be stored and secured as it makes its way through the whole process? And then number three, how [is] that information both shared and accessed?"

The board's study produced recommendations that legislators incorporated into the Student Data Protection Act. This comprehensive bill provides well-defined student data governance protections, restrictions on contracting with third parties, parents' rights to review their students' data, and requirements to seal or destroy potentially harmful data after a certain time — including behavioral records that could follow students indefinitely.

One of the law's most crucial components is a provision requiring the board to "establish advisory groups to oversee student data protection in the state and make recommendations to the board regarding student data protection." As Sallay noted, "Technology moves faster than laws can, so these advisory groups are one mechanism in place to ensure that the law is working and to make further adjustments as needed." The advisory groups ensure that policy decisions reflect the experiences of diverse stakeholders and that policies can be flexible.

Lawmakers used the input from advisory groups in 2017 when the state refined the 2016 law by addressing aspects that were not working as intended. The 2017 legislation improved the consistency of data privacy terms and removed redundant requirements for creating notice and transparency. In addition, it required training on data privacy laws for individuals with access to student records.

What resulted from Utah's due diligence and flexibility was legislation that "basically codified best practices and funded them," said Whitney Phillips, the state board's chief privacy officer from 2016 to 2021. Those best practices — including effective data governance structures, transparency and measures to build local capacity — have earned Utah national recognition for its data privacy efforts.

Utah Student Data Privacy Laws and Rules

Title 53E-9-3: This law requires local education agencies (LEAs) to designate data managers, adopt policies for protecting student data, create data governance plans and establish review processes for external research. The bill also requires LEAs to publish metadata dictionaries, which describe the data the state board collects. In addition, they list ed tech vendors and others who receive student data. LEAs must classify student data as necessary, optional or prohibited and notify parents of their data privacy policies. Schools need parental consent to collect optional data. The bill also requires certain data privacy provisions in all contracts with third-party vendors who use private student data.

Title 53E-9-204: This law requires LEAs to train all employees with access to education records on student privacy laws. Employees must sign a certified statement that they have completed the training and understand student privacy requirements. The agency must maintain a list of employees who have completed the training.

State Board of Education Administrative Rule R277-487: This rule establishes policies regulating data privacy, security, retention and training, including requirements that each LEA provide the state board with its data governance plan, the name and contact information of its data manager and information security officer, evidence of its cyber security framework, and evidence that it has published important information about its data collection and privacy policies. In addition, the rule requires educators to complete annual data privacy training.

Governance: Linking State and Local Decision-making

Utah's far-reaching governance structure is firmly rooted in data privacy protections and extends from the state level to local and school levels. The dedicated chief privacy officer on the state board of education is a keystone in the state's governance structure and privacy efforts and fosters coherence and continuity in efforts to protect student privacy.

Utah understands that good data governance policy is necessary but not sufficient; it must also include support for the people who implement policies at various levels. As Sallay said, "It's not really data governance. Data governance is people governance." At the top level, the chief privacy officer plays a crucial role in connecting and translating among the people who play diverse roles in protecting data privacy. For example, programmers who work in education at the state or local level might not understand how technology or coding decisions can undermine privacy requirements set in law or policy. The chief privacy officer in Utah often ensures that role groups with different skill sets and positions can collaborate to advance student data privacy efforts.

State data privacy requirements also ensure good governance practices at the local level by mandating that LEAs annually provide the state board with a data governance plan and the contact information of the designated data manager and information security officer. According to Utah State Data Privacy auditor Katy Challis, "Having that one focused person in every LEA is really important to managing privacy at [the local] level. And they know that they have a direct conduit to us."

Additionally, the state helped develop governance structures that make data privacy policies easier to follow, including requiring that staff in LEAs have adequate training to ensure they follow data privacy plans.

In responding to data breaches or violations, the state has created structures to help escalate any issues to leadership. Support also exists to communicate the process to people who handle data at the state, district and school levels.

Finally, as Sallay pointed out, data governance in Utah also helps ensure that data privacy requirements are funded. Governance structures break down silos, making it easier to gain an overview of priorities at the state and local levels, and to ensure that funding is requested and allocated for those priorities.

Training and Support: Focusing on the Customer

Utah has some of the nation's most robust data privacy training requirements. The state's 2017 data privacy law requires local school boards to provide training and mandates training for anyone authorized to access education records. To enforce training requirements, it requires each public school to maintain a list of individuals with access to data and requires each school board to certify that each of those individuals has completed training.

Additionally, State Board of Education Administrative Rule R277-487-14 makes data privacy training a mandatory component of teacher relicensure. To support that requirement, it directs the state superintendent to develop student data security training for educators. Teachers who are renewing their educator licenses must now complete the state's interactive online Utah Student Data Privacy Educator Course.

One distinguishing trait of Utah's training requirements, Sallay said, is that the state allows LEAs to adjust their local training efforts to their needs and abilities. While the quality or content of training may differ from one agency or school to the next, state law ensures that there is a minimum standard across the board.

According to Challis, "Instead of nagging people about compliance, we try to be customer service oriented." Utah provides multiple avenues of technical assistance, including dedicated data privacy staff at the state level, help for practical implementation challenges and refresher courses that educators can take when they need them. "We don't exist to tell districts what to do," she said. "We exist to help them do what they need to do."

Transparency: Empowering Families and Students With Information

Transparency is a central component of Utah's data privacy efforts because it empowers families and students to understand and protect their data rights. In addition to publishing data privacy policies on agency websites, Utah strives to make that information actionable for the public. In Sallay's words, "Overwhelming people with information isn't helpful. Parents need to know what's important, and what they can do with this information."

State privacy laws require the state board of education and LEAs to publish information about what data they collect, what benefits and privacy risks those

data collections entail, what they are doing to protect the data, and what rights families and students have over their own data. For example, the state board publishes its Metadata Dictionary, and it requires LEAs to do the same. It posts information about federal and state privacy laws, an interactive list of data privacy agreements with third-party contractors and explanations of state privacy policies.

Just as important, state and local agencies offer clear avenues for parents or families to share concerns or lodge complaints. For example, the state board of education data privacy web pages prominently feature a page where parents can report a privacy concern.

According to Phillips, Utah aims to make it as easy as possible for busy teachers and administrators to take responsibility for privacy: "The state funding helps, but how do we make it easy for the local agencies to care about privacy and make it a responsibility?" Coupled with training and support, she said, "accurate, succinct and entertaining resources are a strategy to get people to care."

Collaborating Across Agencies in Kentucky

Kentucky's deep-rooted culture of data privacy has helped the state become a national leader in education data. One example of its leadership is the Kentucky Center for Statistics (KYSTATS), a state agency that collects, links and reports on education and workforce data so that state leaders, schools and the public can make informed decisions.

Data leaders in Kentucky describe a widespread respect for student data privacy that fosters trust among the state agencies contributing data to KYSTATS. KYSTATS' data privacy policies, practices and resources resulted from collaboration among agencies that focus on early learning, K-12, postsecondary education, the workforce, teacher preparation and health and family services. According to KYSTATS executive director Jessica Cunningham, "Our data systems wouldn't be nearly as successful without our strong agency systems and the security and privacy structures they have created."

Data privacy policies, documents and templates from the Kentucky Department of Education provide the foundation for KYSTATS' data privacy structures and the opportunity for shared learning across agencies. As the department of education's chief data officer DeDe Conner noted of her peer agencies, "We've all copied each other's privacy policies."

Vision: Understanding Why to Collect Data

Education data leaders in Kentucky stress that their data privacy policies are rooted in a clear, public vision for why the data they collect are important. Without such a vision, educators might collect data they don't need or use data in ways no one could have anticipated.

The KYSTATS' security and privacy webpage begins with a statement of value, noting that it "was created to collect, link and evaluate education and workforce data so that Kentucky's leaders, policymakers and the general public can have the facts to make the best decisions for our state." Only then does the page describe how it accomplishes that goal by de-identifying data or suppressing information that can compromise individual students' privacy, among other key practices.

Cunningham explained that KYSTATS' biennial public research agenda underscores the value of the data system by openly addressing such critical questions as, "Why do we want this data? What is its value to the state and its inhabitants?" Answers to such questions can build trust in the communities who provide the data and who stand to benefit most from more informed decision making.

Travis Muncie, who oversees data, research and advanced analytics at the Kentucky Council on Postsecondary Education, described the value proposition at the heart of the state's data systems. He said that every agency, postsecondary institution or student who contributes data to the data system receives something of value in return.

Kentucky education data leaders also emphasize that they do not collect data that serves no apparent purpose. Robert Hackworth, the Kentucky Department of Education's chief information security officer, described his agency's practices as a "data diet." If it isn't required by legislation or doesn't provide something of value to districts or the general public, then the agency doesn't collect it.

Coherent Laws: Respecting a Long Tradition of Data Privacy

State and federal data privacy laws set necessary guidelines for data collection and use in Kentucky, and the state's long-established data privacy culture and practices have built trust. As a result, Conner said, the state does not have

duplicative or excessive data privacy policies and laws: "We don't write a lot of paper in Kentucky. We walk the walk."

One sign of legislators' trust, Travis Muncie noted, is that legislation regulating data privacy at the postsecondary level remains at the "forty-thousand-foot level." In other words, it is not very detailed or prescriptive. This flexibility allows agencies and institutions to adapt to changing technologies and needs.

Kentucky Data Privacy Laws

KRS 160.700-730: This bill requires school officials to protect and preserve all education records and recordings of school activities, inform parents or eligible students of rights to privacy and confidentiality accorded student education records, permit parents or eligible students to inspect and review student education records, and inform parents or eligible students of rights to suppress directory information. It also describes parents' or eligible students' rights to challenge content in student records and governs consent to release student records.

KRS 61.931, .932, .933, .934: This bill requires K-12 schools and postsecondary institutions (along with their contracted vendors), state agencies and nonaffiliated third parties to implement procedures and practices to safeguard against security breaches. This includes notifying officials of such breaches, conducting prompt investigations of breaches, maintaining and updating breach investigation procedures and practices, and establishing procedures for disposing of and destroying records.

KRS 365.734: This statute limits how cloud computing service providers can use student data and prohibits use of student data for commerce or advertising.

Data leaders in Kentucky point to a structural advantage at the department of education: its statewide K-12 data systems make it easier to protect the privacy of student data without additional legislation or controls. Unlike most other states, Kentucky and all of its 171 school districts use the same network and system for keeping track of student information on topics like demographics, course enrollment, assessment results, attendance and grades. As a result, Hackworth said, agency leaders can "see both the forest and the trees." That is, they can keep close tabs on the data privacy and security measures at both the state and district levels.

The statewide system promotes greater coherence of data privacy policy and procedures across the state while limiting opportunities for malicious or unintentional data disclosures. According to Conner, agencies in states without a common student information system must frequently transfer sensitive data among the systems, increasing the risk of inadvertent data breaches.

Governance: Defining Mutually Supportive Structures

Kentucky's nationally recognized education data governance systems support the state's privacy efforts. Data governance structures define the roles and responsibilities that promote clear processes for collecting, storing, sharing, reporting on and destroying student data.

KYSTATS' governance structure establishes checks and balances that protect privacy. Every agency that contributes data to the longitudinal data system reviews that data as it appears on the KYSTATS website to verify that it has been appropriately redacted. Each agency also confirms that KYSTATS is using the data in ways that observe legal requirements and support the partner agencies' shared goals. KYSTATS and its partners revisit their privacy and security policies at least once a year to ensure their relevance to changing conditions.

Such robust governance structures and policies make it easier for KYSTATS to incorporate additional agencies and data systems. KYSTATS director Jessica Cunningham noted that Kentucky's Cabinet for Health and Family Services, the newest partner agency, has multiple data systems and privacy policies that differ from systems in the other agencies. "Our governance structure gives us a track record for how to work through those things," she said, "because we have a process."

Among agencies that govern the system, trust and collaboration fortify the state's data privacy efforts. According to Muncie, KYSTATS' status as an independent agency assures the contributing partners that no single agency will have undue influence on how the system uses state data.

The strength of data governance structures in KYSTATS' partner agencies further supports the state's student data privacy protections. The Kentucky Department of Education's data governance policy describes the purpose, scope, vision and mission of data governance, and it clearly lays out key roles and responsibilities of agency staff. Its guiding principles address privacy head on, balancing "the need for access to data sets" with the need to "protect confidentiality and security of data." One principle for governance gets to

the heart of data privacy: Just because the state has the ability to collect or provide data does not mean that it has the authority to do so. "Always consider key questions," the principle concludes: "Can we? Should we?"

Training and Support: Cementing Diverse Roles and Responsibilities

Governance structures will have little effect on data privacy without comprehensive, adaptable and repeated training for administrators, teachers and anyone else who handles student data. In Kentucky, frequent training on data privacy helps staff in the agencies understand their roles and avoid mistakes that could expose private information.

Every year, KYSTATS trains all staff who use or review data in vital data privacy processes and protocols. For example, they must secure or destroy any sensitive data that could appear in printed materials, email attachments, or files on their computers or other devices. All staff must regularly review Acceptable Use and Data Access and Use policies, and they must immediately bring data security concerns to the attention of the KYSTATS executive director or information systems director.

Partner agencies also conduct data privacy training. According to Conner, her agency provides its staff regular data privacy training and integrates data privacy topics into regular agency events throughout the year, including monthly webcasts or student information system meetings reaching as many as 600 people. The agency's website features best-in-class training resources for schools and districts. The statewide student information system makes it easier to train district and school staff because everyone uses the same system.

Transparency: Keeping Privacy on the Agenda

Kentucky's data leaders promote public trust in data systems by helping policymakers, students, parents and the general public understand how student data is used. KYSTATS publishes its data privacy and security policies, records of its board meetings, its research agenda and a data dictionary, which lists all the data elements it collects.

Partner agencies also publish important information about the data they collect and their policies for protecting that data. For example, the Kentucky Council on Postsecondary Education publishes its data access policy and a set of

comprehensive database guidelines that describe in detail what data the council collects. The Kentucky Department of Education publishes its data privacy and security policies and best practices, offering links to federal and state laws, state data governance policies and best practices for data management.

Data leaders in Kentucky insist that information about data privacy should be part of routine communications with policymakers, families and students. Staff from KYSTATS frequently begin discussions with state leaders by openly addressing privacy and security topics and stressing that data privacy is a priority for the agency. Conner frequently reminds district and school leaders in the state to be similarly transparent with families: "Are you letting your families know what you're sharing, with whom and what you're not sharing?"

Kentucky's data leaders frequently warn about the dangers of data privacy violations. In meetings of state and district administrators and educators, Conner reminds participants that violations of students' privacy can have devastating and lasting consequences for their reputations, opportunities for advancement and financial security. "If you have a data breach," Conner said, "that can impact a child's life."

Final Thoughts

Colorado, Utah and Kentucky each have distinct strategies and priorities for protecting the privacy of student data. Utah's state education agency has a chief data privacy officer, for example, whereas Kentucky splits that role among more than one person. Kentucky's statewide student information system creates a measure of consistency in its data privacy efforts across the state, while Colorado and Utah have policies adapted to more decentralized systems.

However, the states show consistency overall in their adherence to common principles for protecting student privacy. The principles, after all, are not prescriptions. Instead, they offer general guidelines states can follow without compromising their unique policies or neglecting their individual needs. They can help states preserve the power of state education data systems without endangering the students who entrust their sensitive data to those systems.

Acknowledgments

This report is based on research funded by the Bill & Melinda Gates Foundation. The findings and conclusions contained within are those of the authors and do not necessarily reflect positions or policies of the Bill & Melinda Gates Foundation.

About the Authors

Claus von Zastrow

As a senior policy director, Claus works with his Education Commission of the States colleagues to promote timely and relevant education policy and research. He has held senior positions in education organizations for more than 20 years and has spent much of that time helping diverse stakeholders find consensus on important education issues. Claus is dedicated to ensuring that state leaders have the information and guidance they need to make the best possible decisions affecting young people. Contact Claus at cvonzastrow@ecs.org.

Zeke Perez Jr.

As a senior policy analyst, Zeke tracks legislation related to statewide longitudinal data systems, school safety and postsecondary campus safety. He has been with Education Commission of the States since 2014. Zeke has a passion for local politics and enjoys following the varied policy approaches of city and state leaders. Contact Zeke at zperez@ecs.org.