



Leading The Way:

How Six States are Championing Student Data Privacy

by Benjamin Silberglitt, Ph.D., CETL

Introduction

In an era where schools depend on digital tools for everything from instruction to administration, the question of **how to protect student data** has never been more urgent. While federal policies like FERPA and COPPA provide a foundation, they often leave states and districts with more questions than answers.



In most of the country, responsibility for data privacy has fallen to local education agencies (LEAs), leaving them to navigate complex issues with limited resources.

But some states chose a different path. Through legislation, dedicated staffing, or collaborative models, a handful of state education agencies (SEAs) have stepped forward to provide leadership, structure, and support. Over the past two months, I interviewed leaders from six states — Utah, Maine, New York, South Carolina, Mississippi, and Hawaii — to understand the unique conditions that drove their leadership and the lessons they’ve learned along the way.

Utah: Legislation as a Launchpad

Utah’s leadership in student data privacy began with the passage of the **Student Data Protection Act in 2017–18**, which allocated funds and established authority for the State Board of Education to shape data privacy policy statewide. For Katy Challis, Utah’s Director of Privacy since 2022, this legislative backing was essential: “Funding and legislation have been key.” With those resources, Utah has built one of the most comprehensive state-level privacy infrastructures in the nation.

Every district in Utah is required to appoint a **designated data manager** — often a technology leader or registrar — who tracks data flows, oversees privacy, and shares information publicly. While this is

technically an unfunded mandate, it has created a critical network of contacts across the state. The SEA leverages this network with regular communication, bi-annual convenings, and privacy courses offered through Canvas. Over time, this structure has led to a cultural shift: privacy is now part of the conversation in everything from product selection to superintendent reporting.

One of Utah's most impactful strategies has been its strong partnership with the **Student Data Privacy Consortium (SDPC)**. Before SDPC, the legal and logistical burden of contract negotiation fell to individual districts. Now, one district can negotiate a contract and others can "subscribe," dramatically reducing workload. The SEA supports and pays for district participation, ensuring equitable access to this resource.

Another hallmark of Utah's approach is the **careful balance between innovation and risk management**. The State Board of Education takes a cautious stance on data sharing, ensuring student protections remain front and center. Challis and her team help the board weigh risks and benefits — for example, distinguishing between aggregate versus student-level data — so that decisions are both safe and informed. Rather than slowing down innovation, this caution has led to more thoughtful practices and deeper conversations across the state.

Looking ahead, Utah is shifting toward a **new self-assessment model** for districts, asking each LEA to identify privacy goals and report progress annually. This not only holds districts accountable but also promotes continuous improvement. The takeaway from Utah's experience is clear: **strong legislation, sustained funding, and a culture of thoughtful leadership can embed privacy into the DNA of a state's education system.**

Maine: *Building on Relationships and Local Control*

In Maine, where local control runs deep, privacy leadership emerged not from top-down mandates but from **grassroots collaboration**. District leaders had begun working informally on vendor agreements and privacy practices around 2019, but quickly realized they needed state-level coordination. At the request of the alliance of Maine LEAs, the Department of Education jumped in to lend a hand, becoming the state agent for **SDPC** enrollments and providing a backbone of support for districts.

Maine's privacy work is deliberately **team-oriented**. When I asked Director of Education Data Kathy Warren for an interview, she brought along colleagues James Chasse, Technology Infrastructure Specialist, and Alexandra Cookson, Data Quality Trainer. This collaborative spirit reflects their mantra of the **"interoperability of people,"** emphasizing that privacy is not just about technology, but about building human networks of understanding and practice.

The SEA integrates privacy into everything it does, from **webinars on data quality** to discussions about data warehousing and dashboards. A common refrain is the question: “*Can we vs. should we?*” — a reminder that compliance is only the starting point, and ethical considerations must shape decisions about data use. The SEA also provides cybersecurity guidance aligned with NIST and ISO standards, blending privacy with infrastructure and security initiatives.

Maine’s unique history with its statewide **laptop initiative** created a foundation for state presence in schools, particularly in rural areas. This has allowed the SEA to extend its influence into technology procurement, ensuring privacy is part of the conversation whenever state funds support digital tools. Larger districts often get privacy support from groups like TEC (The Education Cooperative), but Maine has focused on ensuring that **small and rural districts are not left behind**.

Challenges remain. Privacy is complex, and many states hesitate to take on the associated risks. Maine’s approach has been to “help, don’t mandate,” recognizing that building trust and capacity is often more sustainable than imposing requirements. The state also sees opportunities for cross-state collaboration, especially around **AI and digital equity**, and has urged **SDPC** to help foster these conversations.

The Maine team’s advice is simple but powerful: **start with consistent messaging, support procurement processes, and never underestimate the power of relationships**. For Maine, leadership is about weaving privacy into the culture of data work while honoring local autonomy.

New York: Rebuilding Trust and Coming Back Stronger

New York’s journey underscores the importance of **trust** in data privacy. The state’s Regional Information Centers (RICs), established in 1967 through a New York State Education Department (SED) initiative, were created to coordinate and standardize IT activities across districts. RICs are divisions of BOCES, known in other states as educational service agencies, that focus specifically on technology and data services. They have long supported school districts and BOCES with technology, data management, and data security.

In the early 2010s, the collapse of the **inBloom initiative**, a project that included New York State, raised widespread concerns about student data privacy. Designed to centralize data and support personalized learning, the project faced strong opposition over issues of transparency and the lack of clear requirements for how vendors could use data and how school districts were expected to protect it. Ultimately, all partner states withdrew by 2014.

In response, New York enacted **Education Law 2-d** in 2014, establishing new requirements for how districts and their third-party contractors and vendors protect data. This legislation elevated data privacy

and security to a new level of importance. It was no longer just a conversation among IT professionals. Teachers, administrators, and district leaders became active participants in shaping how technology is used safely and responsibly in schools. Heather Mahoney, Executive Director of the Mohawk RIC, explained that this legal framework was crucial for reducing shadow use of technology, referring to unsanctioned tools that expose student data to risk.

The RICs began increasing collaboration across the 12 centers to better serve the state, meaning both districts and the Department. By **combining talent** to deliver better support for common needs, they have made that support more effective and cost-efficient. As the RICs recognized the power of working as one under the RIC One brand, and districts leaned into their commitment to tackling work together and sharing resources, New York State began partnering with other alliances and national groups to build on this success. The Student Data Privacy Consortium (SDPC) has played a pivotal role in this evolution by centralizing contract negotiations, creating consistency across districts, and connecting New York's privacy leaders with peers in other states.

New York continues to lead with a strategy rooted in collaboration, transparency, and shared expertise. By fostering a strong community of **trust and cooperation**, the state has built a model for how educational systems can navigate the complexities of data privacy while supporting innovation and learning.

South Carolina: Leadership from a Single Champion

South Carolina's privacy story shows the power of **individual leadership**. For seven years, Felix Childs has served as the state department of education's **Chief Privacy Officer**, slowly expanding the role even without dedicated legislation or a large team. Initially responsible for everything from records management to overseeing security guards, Childs has steadily carved out a space for data privacy as a distinct and vital function.

Working closely with the state department of education's Chief Information Security Officer, Childs has advanced initiatives like **privacy impact assessments**, data classification frameworks, and required district data governance plans. These efforts are now being tied to national standards like the CIS framework, ensuring that guidance is both comprehensive and realistic for districts.

A recent change in administration has provided new momentum, allowing Childs to expand the department's support to districts and prioritize **procurement processes**. By helping all districts participate in **SDPC** — with the state covering costs — South Carolina has increased bargaining power with vendors and provided districts with vetted tools and contracts.

Childs emphasizes that privacy isn't just about incident prevention, but about **protecting the state's most valuable asset: data**. His background in the International Association of Privacy Professionals (IAPP) has brought insights from industries far beyond education, particularly around emerging issues like AI. By framing privacy as central to trust and reputation, he has convinced leadership to see it as a strategic priority.

South Carolina's progress shows that even in the absence of legislative mandates, a committed leader can catalyze statewide change. For other states, the lesson is clear: **start with what you have, connect privacy to existing initiatives, and use every opportunity to raise its profile.**

Mississippi: Privacy as Part of Modernization

Mississippi's privacy leadership emerged as part of a **statewide modernization effort**. When the Department of Education revamped its student information system, privacy, governance, and data quality were built into the design. For Jason Hageman, the Director of IT Security and Data Privacy, this provided a natural entry point to establish privacy as a priority.

Coming from the hospitality and casino industry, Hageman brought a unique perspective: "Privacy is vital there too — your currency is your data." He quickly set out to build trust with districts by positioning the SEA as a **partner, not an enforcer**. His outreach included engaging with technology coordinators, supporting incident response, and participating in statewide groups to ensure schools saw the SEA as a resource.

Despite the absence of privacy legislation, Mississippi has made progress by focusing on **community and relationship-building**, especially in rural districts. Hageman emphasizes empathy and consistency: "What works best is being there by their side when they need it — proving they can count on us." Slowly but surely, this approach has built awareness and improved reporting of privacy concerns.

Mississippi's work is still in early stages, but Hageman is clear that **there's no one recipe for privacy**. Each state must account for its political and educational context. His advice to new leaders is to first "find out what you know and don't know about privacy," and to start with data governance basics. His own learning journey underscores the complexity of privacy in education compared to other industries.

The state's partnership with **SDPC** has been particularly valuable, especially the **National Data Privacy Agreement (NDPA)**, which Mississippi adapted for its own simplified use. Hageman sees opportunities for SDPC to go further, offering frameworks and examples from other states. For Mississippi, privacy is not an isolated initiative but part of ensuring that **every child's education is grounded in both innovation and protection**.

***Hawaii:** Streamlining Privacy Through a Unified & Collaborative System*

Hawaii's approach to student data privacy reflects both its unique structure and its spirit of collaboration. As the only state with a single local education agency (LEA) serving the entire state, Hawaii's Department of Education can coordinate and support schools at a level most states can't match. Yet rather than centralizing all decisions, Hawaii focuses on empowering schools to make their own software choices—backed by strong state-level systems for privacy, security, and quality review.

Over the past six months, Institutional Analyst **Taylor Puuohau** has helped lead an initiative to unify the state's privacy and security review process. Schools will soon be able to submit requests for new software tools through an online helpdesk, where they can also see which systems have already been approved. Vendors seeking approval must agree to the state's standard data sharing agreement, and Hawaii is now working with A4L to transition that standard to the **National Data Privacy Agreement (NDPA)**. Security reviews assess not only data protection but also interoperability, ensuring that tools fit smoothly into Hawaii's digital ecosystem.

Previously, privacy agreements were managed through individual documents—a growing challenge as the number of tools used by schools surged, especially after the pandemic. Today, the state oversees nearly **800 active privacy agreements**, and the move to standardized, trackable contracts has dramatically streamlined the workload. "It's saved us a ton of time," Puuohau said. "Schools feel more secure knowing their data are protected, and they're more eager to participate now that the process is clear and supportive."

A hallmark of Hawaii's approach is the **integration of curriculum leadership** into privacy planning from the very beginning. When designing the new review process, the Department brought together leaders from curriculum, technology, and data privacy—a unique and powerful combination. Curriculum leaders, already deeply engaged with safe and effective classroom use of AI, helped ensure that privacy decisions were grounded in instructional reality. This cross-functional collaboration has made Hawaii's model both practical and forward-looking.

That sense of support reflects how Hawaii's SEA and LEA roles intersect. The single-agency structure gives the department flexibility to act quickly—this new system came together in just months—but Puuohau emphasizes that success also depended on bringing the right people to the table. "Make sure all the right stakeholders are at the table," she advised. "Everyone has knowledge around different aspects of the problem."

For Hawaii, that collaborative mindset, combined with the power of SDPC and the NDPA, has turned a logistical challenge into a model of efficiency, trust, and innovation.

Conclusion: Ingredients for State Leadership

Across these six states, the contexts differ — from Utah’s legislative backing to South Carolina’s single-leader push — but several common threads emerge:

- **Catalysts matter:** whether legislation, a major data incident, or a modernization effort, each state had a trigger for action.
- **Dedicated leadership:** from full teams to lone champions, committed leaders were essential to sustaining progress.
- **Relationships and trust:** building strong ties with districts, vendors, and parents was as important as writing rules.
- **Practical supports:** templates, training, and contract negotiation assistance turned policy into daily practice.
- **Consortiums like SDPC:** shared resources and collective bargaining reduced the burden on districts and elevated state efforts.

These examples show that protecting student data isn’t just about compliance. It’s about leadership, collaboration, and embedding privacy into the culture of education. From Utah’s codified frameworks to Hawaii’s cross-functional teamwork, these states demonstrate that privacy can be both rigorous and responsive. As digital tools continue to evolve, states that take up this mantle will help ensure that innovation in schools is matched with responsibility for the students they serve.

To find out more information about the Student Data Privacy Consortium (SDPC), please visit: <https://privacy.A4L.org>