SEPTEMBER 2022

Utah Leads the Way in Protecting Student Privacy:

A Case Study in K-12 Student Privacy Best Practices

AUTHORED BY

Bailey Sanchez

for the Future of Privacy Forum

*With thanks to **Jim Siegl** for his contributions*

The Future of Privacy Forum (FPF) is a non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. Learn more about FPF by visiting fpf.org.

Table of Contents

Introduction

Though concerns for student data privacy date back to the passage of FERPA in 1974, it has become a central issue as schools have increasingly incorporated education technology into the K-12 learning experience. Effective data use allows parents to track and support their children's progress, helps teachers improve their instruction and tailor it more accurately to students' needs, and helps school and district leaders to make managerial decisions, allocate resources, and communicate with the public. Effectively leveraging technology and student data can improve outcomes for students, but this requires state policymakers to address relevant student privacy issues. Since 2014, state policymakers have worked diligently to address student data privacy concerns – as of 2022, 41 states and Washington, D.C. have passed some form of student privacy law.[1] However, more than carefully crafted legislation is needed to protect student privacy; state policymakers must also provide state boards of education, schools, teachers, and other stakeholders with the resources, expertise, and support to put those policies into practice. Putting the pieces together to protect student privacy can be challenging.

Based on independent research and analysis, as well as interviews with key stakeholders, this case study presents important insights from those who are implementing student data protection efforts on the ground in Utah. Utah sets the bar high for K-12 student privacy. FPF identified the practical steps Utah has taken to establish sustainable, ongoing student privacy practices throughout the state and shares this analysis so that other state policymakers can learn from Utah's efforts to date.

Our exploration of Utah's approach to student data privacy begins in 2015 with the passage of HB 68, which required the Utah State Board of Education (USBE) to make recommendations for updating existing privacy laws. Importantly, this bill tasked the USBE with developing a funding proposal for implementing these changes. The resulting report became the basis for Utah's Student Data Protection Act (SDPA), which went into effect in May 2016. Now Utah's key student privacy law, the SDPA includes governance mechanisms and requirements for local education agencies (LEAs), state education agencies (SEAs), and third-party vendors.

Also key to Utah's long-term success was its decision to fund a Student Data Privacy Office, headed by a chief privacy officer (CPO). Only two other states have a CPO dedicated to student privacy. The office also includes other personnel assigned to student privacy full time, including: a student data privacy auditor, a student data privacy project manager, and a student data privacy trainer. This funding and staffing have allowed Utah to continue to develop and improve upon its privacy program through training, reporting, and resources. In short, Utah's financial investment has enabled dedicated experts and other key stakeholders to implement, follow, and oversee essential student data privacy practices.

Creating a statewide culture of student privacy can be a daunting task. It requires carefully crafted laws, as well as the people and processes to put the laws into practice. It also requires engagement from many diverse stakeholders, including state boards of education, school and district administrators, educators, and parents. Fortunately, Utah's example shows that, by investing in privacy policies, practices, and people, states can create strong and sustainable protections for student privacy.

"The USBE's student data privacy department has not only fostered a culture of student data privacy awareness among educators throughout the state, but it has provided those same educators with a host of helpful resources, trainings, and policies that, when implemented, significantly improve day-to-day student data privacy and security in our public schools."

— PLATTE S. NIELSON, ATTORNEY, ACADEMICA WEST

Summary of Key Utah Student Data Privacy Policies

A short summary of Utah's key student data privacy policies and the main actors involved on the ground in Utah provides helpful context for FPF's analysis of best practices for student data privacy.

Who are the main actors in Utah's student privacy system?

- **SEA**: State Education Agency. Utah State Board of Education (USBE) is Utah's SEA
- **LEA**: Local Education Agency. School districts are at the LEA level
- **State student data officer**: The chief privacy officer at the Utah State Board of Education
- **Student Data Privacy Office**: USBE's department dedicated to student privacy, where the chief privacy officer, student data privacy auditor, student data privacy project manager, and student data privacy trainer work

STUDENT DATA PROTECTION ACT (53E-9-301-309)

The SDPA is Utah's primary student data privacy law. Some of its key provisions include:

- Proactive privacy obligations and procedures that SEAs, LEAs, and third-party vendors must comply with, such as limiting the type of data that may be collected and restricting the ways collected data may be used.
- A requirement that LEAs designate a data manager, who acts as a student privacy point of contact at the local level and is tasked with authorizing and managing data sharing for the school.
- Establishing the role of the state student data officer (or CPO), who, among other things, is responsible for ensuring compliance with student privacy laws throughout the public education system by providing training, support, and resources for data protection at the local level.

STUDENT PRIVACY ACT (53E-9-204)

This law requires each school to create and maintain a list of employees authorized to access education records. LEAs must ensure that each authorized employee is trained, and employees must certify that they completed the relevant training and understand the student privacy requirements. (For more on training, see the section below on Continued Privacy Training).

ADMINISTRATIVE RULE (RULE R277-487-3)

Rule 277-487 in Utah's Administrative Code mandates that each LEA must provide the State Board with the LEA's data governance plan, and the name and contact information of the LEA's designated data manager and information security officer. One person can serve in both roles, or an LEA can designate one person for each role. (For more on the value of providing this information, see the section below on Reporting).

What can we learn from Utah's success?

Based on FPF's research and conversations with Utah's Student Data Privacy Office, Utah's success can be attributed to five main strategies:

- Methodical, collaborative processes to enact change
- Ongoing funding
- Dedicated personnel
- People focused on privacy at all levels
- Privacy is regularly revisited through resources, training, and reporting

Together, Utah's strategies demonstrate best practices for student data privacy. While states may consider adopting one or more of these strategies, our research shows that their combination has been essential to Utah's success, and it is the combination of these five strategies working together that has allowed Utah to build a strong student privacy program.

Utah engaged in ***methodical, collaborative processes to enact change***

To get to where it is today, Utah took a methodical approach to regulate student data privacy. Between 2014 and 2016, protecting student data privacy through legislation was at the forefront of the national privacy conversation,[2] and lawmakers in 49 states introduced nearly 400 student privacy bills.[3] Rather than act rashly to pass legislation in reaction to the political atmosphere of the moment, Utah took over a year to develop student data privacy legislation.

In 2015, Utah passed a bill (HB 68) requiring the USBE to make recommendations for updating student privacy laws and to develop a funding proposal to accompany these updates.[4] The sponsor of the bill, Rep. Anderegg, noted that the bill intended to control what had previously been allowed by vendor requests regarding the collection and use of student data.[5] HB 68 also required the USBE to designate a CPO. The bill included funding for these efforts, which was used to contract an external expert on student privacy to help draft recommendations for student privacy legislation. As the resulting report explains, lawmakers intended that future legislation and guidance from USBE would "provide guardrails within which educators can safely operate with personally identifiable information."[6] The recommended guardrails laid the foundation for Utah's student privacy decisions.

The report was presented to the USBE at a November 2015 meeting and included three major recommendations: (1) development of a data governance plan for USBE and each LEA; (2) creation of data management roles at each LEA with specific responsibilities related to stewardship of personally identifiable information; and (3) funding to support student privacy efforts.[7] Rep. Anderegg attended and explained that the legislature intentionally gave the USBE one year to implement a statewide student data governance plan because it would be a "paradigm shift" that would take time.[8] Many of the report's recommendations ended up in the final Student Data Protection Act, which passed unanimously and went into effect on May 10, 2016.

Taking the time to develop the initial report and recommendations extended the time between the initial call to action on protecting student privacy and when the student privacy law went into effect. However, this step resulted in a collaborative process between the legislature and the USBE. The collaboration process was important in Utah because it ensured that USBE had an active role in the process and was prepared for the task of implementing the law. Including relevant stakeholders in the legislative process can also alleviate unintended consequences by consulting with the parties who will be impacted by the law.

*Utah secured **ongoing funding** to support their privacy program*

Ongoing funding is at the heart of Utah's success on student privacy, and is woven throughout every takeaway in this case study. Conversations with USBE's Student Data Privacy Office revealed their belief in funding as the primary lever that has made a difference in Utah's efforts. As explained by USBE's former CPO Whitney Phillips, "Utah has quickly become a leader in the world of student data privacy because of the resources that have been allocated to the subject. Funding at the SEA level can have profound ripple effects that improve privacy at all levels of education within the state."

Critically, Utah's first bill, HB 68, also required the USBE to develop a proposal to fund student privacy efforts.[9] Typically, state student privacy bills are unfunded. Unfunded legislation may be more difficult to implement when state and local governments facing new obligations without the resources to fulfill them are unlikely to be effective, particularly in the context of protecting student data privacy.[10] Enabling state and local governments to focus on privacy requires ongoing investments of time, money, and resources. The fact that Utah required USBE to develop a funding proposal shows that the legislature understood that recommendations arising from the report would require adequate resources. Although it can be difficult to quantify the return on investment of funded legislation, having resources to establish a chief privacy officer is invaluable. The decision to fund a chief privacy officer at USBE has allowed a full-time, dedicated professional at the state level to operationalize privacy practices.

*Utah's **dedicated personnel** at the state level put policy into practice*

With funding directed toward staffing student privacy positions comes the benefits of dedicated personnel, who act as a bridge between state policy and local practice. As a survey by the National Association of Chief Information Officers on the growing role of state CPOs noted, privacy at the state government level is "complex," and an "enterprise-level privacy official can help bridge the gaps and provide guidance."[11] The report focused on state chief privacy officers, but the sentiment also rings true for those focused on education. Schools collect a plethora of data from students during their education journeys, from demographic information to test scores to teacher observations. To protect this data, schools must comply with federal privacy regulations such as the Family Educational Rights and Privacy Act (FERPA) and the Individuals with Disabilities Education Act (IDEA) in addition to state laws. Different parts of state or local governments may also use student data for many purposes. Privacy law takes time to understand; dedicated personnel are able to become deeply familiar with the legal landscape and navigate the relevant laws.

Utah's law mandates a board of education-level CPO, whose responsibilities include acting as a student privacy point of contact for the state, ensuring compliance,

investigating complaints, reporting violations, and acting as a state-level student data manager. The law also mandates that the USBE designate at least one support manager and a student data protection auditor to assist the CPO.[12] Utah's requirement of a board of education CPO is unusual; to date, only three state laws mandate the establishment of the role.

Privacy is not just about being careful but also about knowing what is permitted within the bounds of the law in order to achieve objectives. Most LEAs do not have attorneys to draft or review agreements. Utah provides assistance to LEAs, who are now able to use an optional template data sharing agreement drafted by the CPO that includes required federal and state provisions. As staff become comfortable with the laws, they can quickly troubleshoot and streamline the compliance process over time. For example, Utah's student data protection auditor checks all required policies and notices, including every LEA's directory information policy. The person in this role has read more than 150 directory policies. The value of this experience is that the auditor can quickly identify common mistakes that LEAs make in their directory information policies, such as leaving "[insert date]" when using policy templates. As David Sallay, USBE's CPO puts it, "We have the time and bandwidth to read these things dozens of times and to know all of those little details that if this was just your part-time job you may not. We can catch the little things because we have the time to know what they are.

In 2016, only the CPO position was funded. In 2017, additional ongoing funding was provided to fund the auditor position. As Phillips explains, "that funding for additional staff would help not just answer questions or provide materials, but provide a follow-up with an auditor."

Because navigating the privacy landscape is challenging and complex, legislators and educators are often unsure of when, how, and with whom they can use student data. States have continued to pass student privacy legislation over the years, but it may be challenging to put policy into practice without the knowledge or resources to understand the law. As Troy Lunt, Technology Director for one of Utah's school districts, reflected, "As the Student Data Privacy Act was passed as law, most of us struggled to untangle the legal language of this new legislation. Fast forward a month and in swoops Whitney, who clearly articulated each requirement and built that foundation of optimism we desperately needed." Having dedicated personnel who spend time understanding the law and its options and implications at the LEA level is vital.

*Utah has **established lines of communication** between the state and local level*

In addition to dedicated personnel at the state level, Utah mandates that a point of contact be designated at each LEA to support ongoing privacy efforts. The relationship between state and local privacy personnel is symbiotic: personnel at the LEA level look to the state for guidance on privacy law and report on activities, and state personnel share resources and support to help ensure that regional and other state personnel are up to date and comply with the law. Additionally, communication from the LEAs helps USBE staff understand what resources should be created to help support privacy initiatives. The law defines the CPO's role as serving as a primary point of contact for student data privacy, ensuring compliance with the law, providing training and support, and producing resources. In working to successfully execute these functions, the CPO builds rapport and develops relationships with points of contact at the LEA level. Relationship-building develops openness to questions. The CPO can

What are some benefits of dedicated student privacy personnel at the state level?

- Deep understanding of privacy laws
- Capacity for technical assistance
- Finding and developing resources
- Assessing, evaluating, and reporting programs and practices
- Building relationships and providing technical assistance

spend time on the ground to understand practical concerns about student privacy and, by maintaining relationships at the LEA level, ensuring that privacy remains a priority. As Whitney Phillips explained, "I understood that privacy was going to be another task for someone within education that was probably already wearing multiple hats. Acknowledging that reality and dedicating my time and my staff's time to reducing that burden on LEAs has encouraged a mutually beneficial relationship."

By developing these relationships, the CPO can build support for the state's privacy goals. Dedicated personnel have expertise on the bounds of the law and can help LEAs accomplish their goals regarding student data. Sometimes schools may have questions about data they would like to collect, and by using the communication system set up through Utah's policies, the CPO can work with the LEAs to determine what the LEAs would like to accomplish and then provide them with potential options.

"Having a CPO at our SEA has provided our Utah professionals with timely and accurate responses to various education privacy questions. Sometimes waiting a day or two for answers can be nerve-wracking, which is why many local education leaders can simply call or text me directly to ask privacy related questions."

— DR. WHITNEY PHILLIPS,
CHIEF PRIVACY OFFICE FOR THE UTAH STATE BOARD OF EDUCATION, 2016-2021

Utah ensures privacy is regularly revisited through ***training, reporting, and resources:***

Data privacy is not just a "one and done," but requires that processes regularly be revisited and refined in order to continue to improve upon existing practices.

Continued privacy training

To keep privacy top of mind among stakeholders, Utah mandates training delivered by both the USBE and by LEAs. The training delivered by USBE is connected to teacher relicensure as a prerequisite to relicensing. Tying privacy training to teacher relicensure ensures regular exposure to student data privacy training beyond what is mandated for new employees. It also ensures training is received from multiple avenues which can help with knowledge retention. USBE's Student Data Privacy Office develops content and resources for trainings, ranging from YouTube videos[13] to training courses for teachers offered through Canvas.

As the chart below shows, some privacy training is delivered at the LEA level. The laws mandating training can be flexible about how training is delivered, and in some cases LEAs can choose to use USBE's resources or another source. Many LEAs ultimately choose to use the Student Data Privacy Office's materials, given the quality of state and federal student privacy resources.

Reporting

Rule R277-487 mandates that each year, LEAs must provide the USBE with the LEA's data governance plan.[14] Additionally, LEAs must designate someone as a data manager and information security officer and provide their names and contact information to the USBE. This ensures that the USBE has a student privacy point of contact for each LEA and facilitates communication between the USBE and individual LEAs. In contrast to the CPO and supporting staff at the state level, however, these designated points of contact are not "dedicated personnel." The data manager and information security officer are often educators whose roles also include acting as a point of contact.

LEAs must also submit their directory information notice, student data collection notice, metadata dictionary, and evidence that the LEA has implemented a cyber security framework. By mandating annual reporting on key elements of LEAs' privacy infrastructure, Utah ensures that privacy remains a priority throughout its K-12 educational network.

Resources

Providing dedicated personnel at the state level reduces the burden on LEAs. Staff who are dedicated to student data privacy full-time can take the time to become familiar with the breadth of existing student privacy resources, such as written materials and developing connections in the student privacy space. Given this deep understanding of the law, dedicated state privacy staff can provide technical assistance at the SEA and LEA levels and can provide answers more quickly than stakeholders might be able to find on their own or by outsourcing.

Dedicated state privacy staff can also support LEAs by providing technical assistance. For example, the Student Data Privacy Office recently helped a school district by clarifying what the law required versus what the district could determine through policy given its specific circumstances. The CPO and supporting team were able to use their experience and expertise to translate the law in an accessible way for local stakeholders.

In general, USBE's Student Data Privacy Office strives to publish materials that are accurate, brief, and somewhat entertaining, in order to keep audiences engaged.[15] They recognize that teachers

Trainer	Training	Audience	Frequency	Source of requirement
USBE	Data security and privacy training	Licensed educators	When re-licensing	Utah Admin. Code R277-487-9 (2019)
LEA	Confidentiality of student data	Any employees with access to education records as defined in FERPA	Annually	Utah Admin. Code R277-487-3(8) (2019)
LEA	Training on student privacy laws	Any employee who will have access to education records as defined in FERPA	Before an employee can be authorized to access education records	Utah Code § 53E-9-204(3)

are busy and student data privacy is a small part of their job rather than something they actively think about every day. By developing resourves that can be used throughout the state, USBE has helped shift the burden to those who can dedicate their time and expertise to student data privacy, rather than having each LEA develop its own resources. The communication structure created by the law's requirements also creates a feedback loop for resource creation. State staff remain informed on issues raised by LEAs, which are then incorporated into future trainings and resources.

"At times, it seemed that full compliance was a pipe dream. Between all the legal requirements, data governance (including data privacy and security), and training, there seemed to be so much 'stuff.' USBE was keenly adept at recognizing where local education agencies would require the most help. They proactively created resources (templates and videos), and introduced the Student Data Privacy Consortium SDPC for districts to manage their own data privacy agreements. USBE support made the impossible very possible."

— TROY LUNT, TECHNOLOGY DIRECTOR, IRON COUNTY SCHOOL DISTRICT

Conclusion

As states continue to grapple with student privacy issues, FPF has identified Utah as an important model for student privacy best practices. Not only has Utah thoughtfully passed legislation, but stakeholders have also implemented the law in a practical way. Utah decided to invest money in student privacy, and that investment has brought people who have the capacity to implement, follow, and oversee processes.

States seeking a starting point for their own student privacy journeys should consider following Utah's thoughtful approach of first funding a small study by experts and key stakeholders in order to inform more comprehensive legislation like the Student Data Privacy Act. Beginning with a study, report, or another pilot can be a low-risk commitment for a legislature and a strategy to introduce legislation that requires participation from multiple stakeholders. Other potential steps to success could include designating people in each district to be responsible for data privacy, establishing communication between the state and local level, or placing a greater emphasis on training, reporting, and resources.

Ultimately we attribute Utah's success to a combination of sound student privacy strategies and best practices. Other states have adopted parts of Utah's model but have not had the same level of success. Utah's initial investment in a Student Data Privacy Office has allowed it to continue to build best practices and emerge as a leader in state student data privacy.

Endnotes

1 Student Privacy Compass, State Student Privacy Laws, Accessed March 1, 2022, https://studentprivacycompass.org/state-laws/.

2 Tanya Roscorla, States Broaden the Student Data Privacy Conversation with 2016 Legislation, Center for Digital Education, (March 25, 2016), Accessed February 22, 2021, https://www.govtech.com/education/k-12/States-Broaden-the-Student-Data-Privacy-Conversation-with-2016-Legislation.html.

3 Brenda Leong, Linnette Attai, Amelia Vance, and David Rubin, FPF Guide to Protecting Student Data Under SOPIPA, Future of Privacy Forum, (2019), Accessed February 18, 2021, https://fpf.org/wp-content/uploads/2016/11/SOPIPA-Guide_Nov-4-2016.pdf.

4 Student Privacy Study, Utah H.B. 68, 2015 General Session.

5 Utah State Board of Education, Meeting Minutes, (April 9-10 2015), Accessed April 8, 2021, https://www.schools.utah.gov/File/b9d6e62e-9273-4ec1-abef-cf58c07d7fe9.

6 Glynn Ligon, Steven King, and Barbara Clements, Recommendations and Funding Proposal to Further Improve or Enact High-Quality Practices and Supports to Safeguard Student Personally Identifiable Information, ESP Solutions Group, (December 4, 2015), Accessed February 18, 2021, https://le.utah.gov/interim/2016/pdf/00000451.pdf.

7 Utah State Board of Education, Meeting Minutes, (November 5-6 2015), Accessed February 2, 2021, https://www.schools.utah.gov/File/3547b490-1feb-4c56-a18a-339d4fed851e.

8 Utah State Board of Education, Meeting Minutes, (November 5-6 2015), Accessed February 2, 2021, https://www.schools.utah.gov/File/3547b490-1feb-4c56-a18a-339d4fed851e.

9 Student Privacy Study, Utah H.B. 68, 2015 General Session.

10 Jules Polonetsky, Amelia Vance, and Bill Fitzgerald, Securing Student Data Is a Challenge that Requires Sufficient Funding, The Hill (December 4, 2017), Accessed February 23, 2021, https://thehill.com/opinion/cybersecurity/363095-securing-student-data-is-a-challenge-that-requires-cash.

11 National Association of State Chief Information Officers, Perspectives on Privacy: A Survey and Snapshot of the Growing State Chief Privacy Officer Role, NASCIO, Accessed February 18, 2021, https://iapp.org/media/pdf/state_chief_privacy_officer_perspectives.pdf.

12 Utah Code § 53E-9-302(5).

13 USBE Student Data Privacy, Metadata Dictionary Tutorial, YouTube video (February 9, 2021), Accessed April 27, 2021, https://www.youtube.com/watch?v=YRfiU9owBAk; USBE Student Data Privacy, Utah Law Student Data Protection Act, YouTube video (February 9, 2021), Accessed April 27, 2021, https://www.youtube.com/watch?v=2uEfp1WqJDg.

14 Utah Admin. Code R277-487-3 (2019).

15 USBE Student Data Privacy, FERPA Exceptions, YouTube video, (February 12, 2021), Accessed February 18, 2021, https://www.youtube.com/watch?v=bHbt96phFqU; USBE, Utah Student Data Privacy Educator Course, Accessed February 18, 2021, https://usbe.instructure.com/courses/75; USBE Student Data Privacy, Oct 1 2020 Compliance Check, Webinars, (January 20, 2021), Accessed February 18, 2021, https://www.youtube.com/watch?v=KdFWI7Lmwtk&list=PLLqKrGVGr6pRbwa8pjrv77UiU0Q5AxNW7&index=3.

1350 EYE STREET NW | SUITE 350 | WASHINGTON, DC 20005 FPF.ORG | info@fpf.org