NCSL
NATIONAL CONFERENCE OF STATE LEGISLATURES

Scott Bedke
Speaker of the House
Idaho
President, NCSL

Anne Sappenfield
Director
Legislative Council
Wisconsin
Staff Chair, NCSL

Tim Storey
Chief Executive Officer
NCSL

Student Data Governance

To facilitate the use of educational data in decision-making, states have established student data governance systems to ensure data security and privacy for student information. The Data Quality Campaign, a nonprofit policy and advocacy organization focusing on supporting state development of education data systems, describes data governance as an institutionalized structure that "define[s] the roles and responsibilities needed to ensure clear processes for collecting and reporting education data and to ensure accountability for data quality and security."[1] State legislatures play a pivotal role in creating that structure by providing direction and support for student data governance.

Legislative Role in Student Data Protection, Retention and Safety

Education data legislation governs the lifecycle of data, creating the policy conditions for the collection, protection, and use of state data. Best practices around state education data governance laws include:

- Explicitly setting the purpose of the state's privacy laws in the context of the importance of collecting and reporting educational data
- Assigning responsibility for developing and implementing policies, providing guidance, and sharing best practices with local education agencies
- Establishing a public data inventory with a description of each data element
- Providing for the development of a statewide data security plan that establishes minimum data privacy and security compliance standards, requires regular compliance audits, requires breach notification and mitigation procedures, and identifies storage and security protocols
- Promoting transparency and public knowledge of data related policies and available reports
- Providing sufficient funding for initial implementation and ongoing technical assistance.[2]

Establishing the purpose of the state's data privacy laws while acknowledging the importance of data collection and reporting sends a clear message of state priorities to the public and administering agencies. By grounding data protection in the need for educational data, the legislature can emphasize the importance of data driven decision-making as the driver of student data governance. For example, Colorado House Bill 1423 (2016) states:

> The general assembly recognizes that, with the increasing use of technology in education, it is imperative that information that identifies individual students and their families is vigilantly protected from misappropriation and misuse that could harm students or their families. The general assembly also finds, however, that there are many positive ways in which a student's personally identifiable information may be used to improve the quality of the education the student receives and to positively impact the educational and career outcomes that the

[1] Data Quality Campaign. (2018, January 30). *A Roadmap for Cross-Agency Data Governance: Key Focus Areas to Ensure Quality Implementation*. https://dataqualitycam.wpenginepowered.com/wp-content/uploads/2018/01/DQC-Cross-Agency-Gov-Roadmap-02042020.pdf

[2] EducationCouncil LLC. (2014, March 3). *Key Elements for Strengthening State Laws and Policies Pertaining to Student Data Use, Privacy, and Security: Guidance for State Policy Makers*. https://educationcounsel.com/?publication=key-elements-for-strengthening-state-laws-and-policies-pertaining-to-student-data-use-privacy-and-security-guidance-for-state-policymakers
Data Quality Campaign. (2021, December 7). *Principals for Education Data Legislation: A Checklist for State Legislators and Staff*. https://dataqualitycam.wpenginepowered.com/wp-content/uploads/2021/12/Principles-for-Education-Data-Legislation.pdf

> student achieves. The general assembly finds, therefore, that student data can be both protected and positively applied by increasing the level of transparency regarding, and specifying and enforcing limitations on, the collection, use, storage, and destruction of student data.

Assigning individuals or organizational bodies with specific responsibilities around student data governance facilitates systems management as well as provides a mechanism for accountability. Some states require a chief privacy officer or governing board, while others vest responsibility in the state board of education or state department of education more generally. In West Virginia, statute directs the state's department of education to:

> Create, publish, and make publicly available a data inventory and dictionary or index of data elements with definitions of individual student data fields in the student data system to include [and] Develop a detailed data security plan that includes:
> (A) Guidelines for the student data system and for individual student data including guidelines for authentication of authorized access;
> (B) Privacy compliance standards;
> (C) Privacy and security audits;
> (D) Breach planning, notification and procedures;
> (E) Data retention and disposition policies; and
> (F) Data security policies including electronic, physical, and administrative safeguards, such as data encryption and training of employees.[3]

For states with state longitudinal data systems (SLDS), governing boards help facilitate cooperation and coordination between relevant state agencies and stakeholders. Using legislation to establish such governing boards as independent agencies creates a sustainable structure that allows for cross-agency data governance.[4]

Ensuring the availability of sufficient resources provides responsible parties with the organizational capacity to fully implement and sustain data governance structures.[5] States can also set aside funds for agencies to support local education agencies in protecting student data. Virginia, for example, requires the state's department of education to:

> designate a chief data security officer, with such state funds as made available, to assist school divisions, upon request, with the development and implementation of their own data security plans and to develop best practice recommendations regarding the use, retention, and protection of student data.[6]

In addition to these individual policy examples, the Future of Privacy Forum, a nonprofit organization focusing on data privacy and emerging technologies, recently highlighted Utah's overall approach to student data privacy. They found that legislation in Utah has been successful in protecting student data privacy by providing for collaborative processes to enact change, ongoing funding, dedicated personnel, and regular revisitation of privacy through resources, training, and reporting.[7]

Data Retention and Destruction

State statutes generally do not include the specific procedures for data retention and destruction, rather directing state boards of education or state departments of education to establish and maintain such requirements. Doing so provides

---

[3] W. Va. Code Ann. § 18-2-5h

[4] Data Quality Campaign. (2018, January 30). *The Art of the Possible: Cross-Agency Data Governance Lessons Learned from Kentucky, Maryland, and Washington*. https://dataqualitycam.wpenginepowered.com/wp-content/uploads/2018/01/DQC-Cross-Agency-Gov-CaseStudy-090920.pdf

[5] Data Quality Campaign. (2011, July). *Supporting Data Use While Protecting the Privacy, Security, and Confidentiality of Student Information: A Primer for State Policymakers*. https://dataqualitycampaign.org/wp-content/uploads/2016/05/Supporting-Data-Use-While-Protecting-Privacy-Primer.pdf

[6] Va. Code Ann. § 22.1-20.2

[7] Sanchez, Bailey. (2022, September 19). *Utah Leads the Way in Protecting Student Privacy: A Case Study in K-12 Student Privacy Best Practices*. Future of Privacy Forum. https://studentprivacycompass.org/resource/utah-case-study/

the flexibility for continual updates to state requirements to keep pace with evolving technological opportunities and challenges.

Regarding third party vendors, many states have provisions that dictate the requirements for the retention and destruction of student data as well as allowable uses of the data. Some specify the destruction and retention policies that third parties must follow, while others require the agreements between local education agencies and third parties establish destruction and retention policies. For example, Delaware requires third party operators to delete student data within 45 calendar days upon request from the local education agency, while Louisiana requires that contracts between local education agencies and third party operators include requirements for information storage, retention, and disposition.[8] Provisions for third party operators' use of data frequently include disallowing for targeted advertising and selling of student data.

Student Data Protection Assistance

In addition to the training, guidance, and resources that states may provide for, the U.S. Department of Education established the Privacy Technical Assistance Center (PTAC) to provide information and guidance related to student education data. PTAC releases informational resources, training materials and videos, and best practices for data governance and security for a variety of stakeholders, including local education agencies, parents, and students.[9]

Trends[10]

During the most recent legislative session, 131 education data bills were introduced in 35 states, 42 of which became law in 17 states. One of the most prominent trends across these legislative efforts was provisions to make new or existing state data available to students, families, and the public. Additionally, several states looked to disaggregate their student data by a variety of student characteristics to better understand differences in student experiences and areas of need.[11] Legislative efforts around cybersecurity have also been increasing, with a range of initiatives proposed around improving governance and technical assistance, and requiring training for contractors, and improving security practices.[12]

Specifically concerning student data privacy, increasing attention is being given to educational software and including stakeholders in decision making. Such efforts can occur in tandem; for example, Maryland recently enacted Senate Bill 325 (2022), which codified recommendations from a formalized stakeholder group to expand the definition of protected information to include students' online behavior and persistent unique identifiers generated through use of digital technologies.

Overall, these trends highlight the ability of state legislatures to establish, support, and maintain student data governance systems that protect student information while promoting data-driven decision making.

---

[8] Del. Code Ann. tit. 14, § 8104A; La. Stat. Ann. § 17:3914

[9] Protecting Student Privacy: A Service of the Student Privacy Policy Office's Privacy Technical Assistance Center. U.S. Department of Education. https://studentprivacy.ed.gov/

[10] For a list of state laws pertaining to student data privacy, Student Privacy Compass provides a searchable database of state student privacy laws on their website: https://studentprivacycompass.org/state-laws/. NCSL's Education Legislation Bill Tracking searchable database (https://www.ncsl.org/research/education/education-bill-tracking-database.aspx) also houses enacted legislation pertaining to data.

[11] Data Quality Campaign. (2022, October 11). *Education Data Legislation Review 2022*. https://dataqualitycampaign.org/resources/flagship-resources/education-data-legislation-review-2022/

[12] Consortium for School Networking. (2021, December). *2021 State and Federal Cybersecurity Policy Trends: Insights for Education Technology Leaders & Policymakers*. https://www.cosn.org/cosn-news/cosn-reveals-2021-k-12-cybersecurity-policy-trends-in-new-report/