Roadmap to Safeguarding Student Data

Key Focus Areas for State Education Agencies

DATA FOR ACTION

Why are we going on this road trip?

If our destination is improved student achievement, we cannot get there without valuing and effectively using data in education. Central to reaching this goal is building trust among all those who have a stake in education that individual student data, such as attendance, course taking, grades, and test scores, are being collected for meaningful purposes and kept safe, secure, and private.

Safeguarding student data is not just a technical project done by one person within the state education agency (SEA). It must be an integral part of the SEA's purposeful, planned, and transparent efforts to use data in support of student learning. This is about changing the culture in the SEA around data, and this culture change starts from the top. Safeguarding student data needs to continue to be a priority of SEA leadership, and the SEA needs to effectively use and protect student data.

Far from being a detour, safeguarding student data is a critical component of effective data use. When SEAs create high-quality policies and practices that govern data protection and use, they can be confident they are on the right path to using data to answer critical stakeholder questions and to inform decisions to support continuous improvement. By implementing these policies and practices, SEAs can engage everyone who works with data in a culture of valuing data, clearly communicating about data, and understanding and practicing ethical data use. This roadmap is designed to help SEAs improve both the specific policies and processes to safeguard data and the transparency and communication practices needed to create this responsible data culture.

Where are we going?

Having a high-quality student data privacy policy and implementing related supporting practices allow SEAs to meet their legal, technical, and moral obligation to safeguard the student data they collect and use to support student achievement. Through privacy policies, data governance processes, and ongoing communication, states describe and codify the procedures, personnel supports, and data collection and use guidelines that SEAs employ to safeguard the state's education data. Making student data privacy policies publicly available provides transparency around data use, helping build trust with the public that student data are being collected, managed, and used in responsible and ethical ways. Supporting practices, such as data privacy training for SEA staff, awareness building, and communication processes, ensure that the privacy policy is implemented effectively and consistently by the SEA staff who are entrusted with student data.

Every SEA must create and continuously update high-quality student data privacy and confidentiality policies and develop supporting governance structures and practices, which prescribe how student data are used and protected in the service of improving student achievement. This document provides specific, practical recommendations for SEAs as they prioritize the safeguarding of student data and continuously review and update their data privacy policies and practices to address changes in technology.

How do we get there?

All SEAs—and everyone who works with student data—must comply with the Family Educational Rights and Privacy Act (FERPA) and other federal and state laws that protect the privacy, security, and confidentiality of student data. However, to enhance the safeguarding of student data and to address local needs and contexts and the evolving use of technology in schools, SEAs should develop their own data governance structures and processes as well as a publicly available student data privacy policy. SEAs can also enact high-quality practices and supports to safeguard student data by focusing on three key areas:

1. **Transparency:** Clearly communicate internally and with the public about the policies and procedures designed to protect student data and about how data are collected, used, and safeguarded.
2. **Governance:** Design structures and delineate roles and responsibilities that establish stable procedural and personnel-based supports for the effective implementation of privacy policies.
3. **Data Protection Procedures:** Implement specific security and privacy strategies, processes, and controls that physically, technically, and legally safeguard student data.

Tools for the Trip

Find additional resources from the Data Quality Campaign (DQC) and other organizations to aid in developing and implementing SEA student data privacy policies and practices, including the following:

- guides on talking about data with different audiences
- guidance and technical resources for state policymakers
- practical tools for crafting legislation to safeguard and govern data and for selecting and working with service providers

Planning Ahead for Future Journeys

As SEAs develop high-quality policies and practices to protect the data they collect and use and recognize the importance of data quality and integrity to support student achievement and enact critical reforms, they can also begin to consider additional ways to strengthen their privacy policies and practices and create a culture of shared commitment to responsible and effective data use, such as

- identifying ways to share information about current data uses and research studies with parents and other members of the public;
- using findings from risk assessments (internal review of existing privacy policies and practices) and security audits (internal or external review of processes and technical environment) to strengthen and formalize student data privacy policies and procedures;
- implementing SEA policies and establishing practices for public transparency around how student data privacy policies are developed and implemented;
- identifying elemental-level data that contribute to student level indicators, and determining appropriate protections for each element (e.g., identifying the exact data pieces used to calculate a student's record of chronic absence); and
- creating a policy or process that addresses the commercialization of student data. While states are legally prohibited from selling student data, they bear a responsibility in defining the permissible collection and uses of data by external technologies and programs used in classrooms.

Together, these recommendations can guide state efforts to continually adapt, revise, and refine their data privacy and security policies and practices. Ultimately, however, policies and procedures are only one part of the larger effort to transform the culture of education data use from one of accountability to one of providing meaningful services and high-quality education to every student. Hopefully, SEA efforts to engage state leadership in data governance, codify processes, and communicate with other agencies and the public will support this culture change and keep states moving down the road of using data ethically and effectively to support students.

FOCUS AREA 1

Transparency

Transparency refers to the clarity and availability of the SEA's materials and communication around the collection, use, and safeguarding of student data. Materials can include the SEA's privacy policy, inventories of data collected by the state and how they are used, and lists of external data requests. Communication refers both to internal SEA communication structures and to outreach activities to the public.

How does transparency safeguard student data?

Transparency around privacy policies and practices is critical to building trust with the public, particularly parents, about the value of data. If the public is confident that the data collected are safeguarded and are used in specific, ethical ways to help students succeed, they can trust the SEA to collect and use student data. In addition, seeking public participation, discussion, and input on the use of data and its governance fosters empowerment and builds collaborative relationships with parents, teachers, and education leaders.

What does transparency look like?

STUDENT DATA PRIVACY POLICY

- Relevant state, local, and federal laws are referenced in the SEA student data privacy policy.
- There is an annual or regular review and update of the student data privacy policy.
- The student data privacy policy clearly states the types of student data collected and the purposes for which the data will be used, and it refers to data protection, maintenance, and rentention procedures.
- The student data privacy policy is publicly available and no more than one click away from the SEA website homepage.
- The student data privacy policy is available in additional languages or formats (depending on the state population).
- The student data privacy policy is clear and written in plain language, not technical or legal terminology.
- The student data privacy policy contains protocols for sharing data (e.g., with researchers, nonprofit partners, other state agencies).

WRITTEN RECORDS

- There is a data inventory or data classification (e.g., a data dictionary) that defines each data element collected and stored by the SEA that is regularly reviewed and updated.
- The SEA maintains and publishes a list of all external student data requests that are fulfilled and indicates what data were provided and whether the requests included personally identifiable information (PII) that could be used to identify an individual student.

FOCUS AREA 1

COMMUNICATION

- There is a written internal communication structure, providing clarity around when and how to include executive-level staff in critical conversations.
- There is a clear and documented process for receiving and responding to complaints, concerns, and questions from parents and other individuals about the privacy policy or the use of student PII.
- There are processes for engaging internal and external stakeholders (e.g., SEA department heads, state information technology office) to gather feedback about the privacy policy.
- The SEA solicits broad public comment on the privacy policy with clarity around which issues are open for public comment and which are not.
- Information is available for parents and other internal and external stakeholders to explain the student data privacy policies (e.g., through brochures, flyers).

How can an SEA achieve this?

SEAs can create a clear, user-friendly place on their websites that allows members of the public to easily access the student data privacy policy and understand how the SEA safeguards student data. SEAs can also prepare a description of the uses of the data and the benefits for families, teachers, and schools. State leaders should be able to speak to the value of data in supporting student achievement in the state and how the SEA safeguards student data through the SEA's privacy policies and practices.

FOCUS AREA 2

Governance

Data governance, a critical aspect of data management, provides the SEA an opportunity to define and establish the roles and responsibilities needed to institutionalize a commitment to data quality and use. Without a data governance strategy there is no clear ownership of the data; no clear business processes for collecting, managing, and reporting data; and no accountability for data quality and integrity.

Governance is needed to ensure that integrated and master data (data which are collected once but used in numerous places) are used and disclosed only for proper purposes and in the proper manner. In addition, governance structures can ensure that the state collects and uses data effectively to answer critical questions about student achievement and school performance and to identify best practices and pathways for student success. Governance related to safeguarding data can include establishing training and supports for SEA personnel, defining roles and responsibilities around internal auditing and accountability, and delineating standards for contractors and vendors who have approved access to limited student data.

How does governance safeguard student data?

Data governance is needed to establish the best structure and identify the right individuals to make decisions and implement the SEA's education data collection and use framework. Governance empowers these bodies and their members with the authority and responsibility to make necessary decisions that ensure data are used effectively and in compliance with the state's privacy policies and practices (and to create consequences for noncompliance). In addition, governance gives sustainability to these policies and practices and ensures that they will safeguard student data over time, even as leadership priorities change.

What does governance look like?

STAFF SUPPORTS

- There is executive-level (e.g., chief state school officer) support for data governance.
- There is a chief privacy officer or other high-level official who plays a significant role in the SEA's privacy efforts (i.e., this is an official position or an explicit component of a job description).
- The SEA has or supports a program to increase awareness of privacy policies and practices among its staff.
- There is ongoing professional development and training for SEA staff on safeguarding student data, including new protocols, issues, and policies. SEA staff are required to complete training on a regular basis (e.g., annually), measure their understanding, and are responsible for achieving a specified threshold in regard to training standards. Not meeting this threshold has consequences, including denial of access to data.
- The SEA works with its human resource department to incorporate employee responsibilities around safeguarding student data into position descriptions, especially those dealing with confidential information.
- There are efforts to further develop the skills of the SEA staff to safeguard student data (e.g., external conference attendance, group discussions of whitepapers, webinars).

FOCUS AREA 2

INTERNAL ACCOUNTABILITY PROCESSES

- Data requests are handled using established data governance procedures.
- There are documented data system and compliance audit processes, and they are reviewed and updated at least annually.
- There are reviews of privacy implications associated with new data sharing or analysis opportunities.
- There are documented rules for disclosure avoidance (i.e., processes to avoid unintentionally releasing PII) before publishing data (in accordance with FERPA), and they are reviewed and updated at least annually.

CONTRACTING AND DATA SHARING STANDARDS

- If student data are shared with third parties (e.g., researchers, evaluators), the sharing is done in compliance with federal, state, and local laws.
- There is student data privacy policy and data governance orientation, which is required for contractors and vendors who have approved access to limited student data.
- Memoranda of understanding for cross-agency data sharing (e.g., between the SEA and in-state postsecondary institutions) include processes that follow all relevant state, local, and federal data privacy laws. These processes include appropriate monitoring provisions for all long-term or renewable data sharing agreements.
- External contracts satisfy all applicable privacy laws. These contracts minimally include data protection responsibilities required of contractors and vendors that are comparable to those required of SEA staff who have approved access to student data. The SEA monitors contractor and vendor capability and follow-through to protect student data.

How can an SEA achieve this?

SEAs can support their implementation of high-quality data governance to safeguard student data by responding to data privacy conversations within the state and ensuring that governance structures and procedures address this context. This may include responding to specific public concerns (e.g., the use of a service provider, teacher effectiveness policies) or working with other state entities participating in data governance work, such as state school boards or state executive leadership. SEAs can also address the implications of changing data management technologies (e.g., cloud computing, mobile devices, new data management applications and software) through their governance procedures.

FOCUS AREA 3

Data Protection Procedures

Data protection procedures are the formalized, internal activities and standards that SEAs employ to manage and protect the education data they collect.

How do data protection procedures safeguard student data?

Data protection procedures ensure that the SEA has specific protocols and supports in place to safeguard student data. These procedures are formalized, documented, and regularly shared internally. They include measures to physically safeguard data; to ensure the proper orientation, training, and monitoring of staff interacting with data; to implement formal student data privacy policies at the state level; and to create procedures to ensure that data are protected across multiple uses (e.g., research, evaluations, public reporting).

What does data protection look like?

PRIVACY AND SECURITY PROCEDURES

- The SEA develops and implements comprehensive and effective physical, technological, environmental, and legal data privacy and security policies and procedures. Policies and procedures address the following:
  - the encryption, storage, and transmission of student PII
  - disclosure processes that describe the appropriate situations and processes for releasing or sharing student data
  - personnel management and training for staff who have access to student data
  - processes for data destruction in all places where the data are stored
  - procedures for tracking and monitoring processes and activities to ensure that they are followed and consequences for not doing so (e.g., data destruction practices are monitored to ensure data were destroyed as specified)
- Levels of data sensitivity are clearly defined, and data are categorized by these levels, with appropriate differences in levels of protection depending on how sensitive the data are. The definitions and categorization should recognize that although all student data may be considered sensitive, some pieces of data (e.g., special education indicators) may be considered more sensitive than other pieces of data (e.g., attendance rates).
- Processes and practices ensure that encryption or other protection is in place during movement or transmission of sensitive or confidential data and that these protections are routinely reviewed and kept up to date.

PERSONNEL

- SEA staff annually review the student data privacy policy and provide written assurances that they will meet their data privacy responsibilities as a prerequisite to getting access to data.
- There is orientation for new SEA staff regarding data responsibilities soon after beginning employment and for current SEA staff with new responsibilities; access to data depends on completion of the orientation.
- Access to student PII is based on SEA staff roles and responsibilities. There is a regular audit, conducted at least annually, of the responsibilities of continuing SEA employees to ensure that data access levels remain appropriate. Data access privileges are updated when SEA staff take a new position in the agency, new SEA staff join, and SEA staff leave.
- Background checks are performed on SEA employees who have access to student PII.

FOCUS AREA 3

POLICIES

- There is a documented data retention policy that explicitly addresses for how long and in what manner student data should be kept to ensure its availability for legitimate educational purposes while safeguarding student data.
- There are documented processes around the use of PII data for software application development and related processes (e.g., helpdesk support, troubleshooting issues).
- There is a regularly reviewed list of approved vendors who have appropriately authorized access to student data for legitimate educational reasons. Appropriate agreements are in place with vendors and are monitored and updated.
- There are documented policies regarding data ownership and appropriate uses of shared data. These policies include consulting with data owners (i.e., the agency that initially supplied the PII and has primary responsibility under law for its proper use and protection) about other potential uses of the data.
- Documented roles and responsibilities regarding data protection, data ownership, and data access are regularly reviewed and updated.
- There are documented policies for handling privacy incidents, such as data breaches, including a response process with designated leadership. Privacy incidents are tracked in a standardized way, and the public is notified when appropriate.

PROCESSES

- The SEA or another state agency conducts a periodic risk assessment (a review of existing privacy policies and practices leading to an identification of potential privacy risks), and findings are documented and tracked to ensure that appropriate action is taken to resolve identified risks.
- For all personally identifiable student data sets, there are test data (data that cannot be linked or traced to actual individual students) available for application testing, demonstrations, trainings, etc.
- There is a process to determine the educational needs that require collection, maintenance, or disclosure of data (both within and outside the SEA). That is, the SEA can articulate why student data are being collected or shared (e.g., to improve student achievement, to comply with laws and regulations).
- There is a documented process for submitting, authenticating, and evaluating external data requests. This process includes steps to determine whether internal and external requests for data can be adequately met with de-identified or aggregate data rather than PII.
- There are data minimization processes to ensure that data elements are collected, maintained, and/or linked only when needed for specified purposes.
- There are practice drills and process reviews for privacy incidents (e.g., data breaches) to ensure that processes and procedures are effective and being followed appropriately.

How can an SEA achieve this?

SEAs can review their existing data privacy policies, and policies across state agencies, to ensure that the SEA student data privacy policy is consistent with other state policies (e.g., in terms of governance, penalties, and personnel, such as having a chief privacy officer). States can determine gaps and inconsistencies or overlaps among the state privacy policies and create an SEA student data privacy policy that complements and is consistent with other privacy policies in the state.

TOOLS FOR THE TRIP:
Additional Resources from DQC and Other Organizations on Safeguarding Student Data

Value of Data

- Ms. Bullen's Data Rich Year: This graphic follows a teacher and student through the school year to see how data help teachers, parents, and others make sure students are meeting education goals.

Communicating about Data

- Talking about the Facts of Education Data with Policymakers: This one-page fact sheet answers critical questions for policymakers about the federal role in data collection and regulations prohibiting the selling of student data.
- Talking about the Facts of Education Data with Parents: This one-page fact sheet answers critical questions for parents about why states and districts collect education data and what the federal role in data collection is.
- Talking about the Facts of Education Data with School Board Members: This resource, created in conjunction with the National School Boards Association, is designed to help school board members better understand the value of education data and their role in safeguarding student data.

The Facts about Safeguarding Data

- Myth Busters: Getting the Facts Straight about Education Data: This set of myth busters provides facts about common education data misconceptions, including the perceived federal role in data collection, sensitive student information, and FERPA.
- Safeguarding Student Data: This one-page fact sheet outlines three strategies for policymakers to pursue in their efforts to safeguard student data and support effective data use: addressing stakeholder needs, communicating with the public, and implementing appropriate policies.
- Communicating Data Toolkit: This toolkit contains language and tools for talking with peers, press, and the public about data and meeting education goals.

Guidance and Technical Resources for Policymakers

- Supporting Data Use While Protecting the Privacy, Security and Confidentiality of Student Information: This publication outlines three overarching responsibilities of state policymakers to protect the privacy, security, and confidentiality of students' PII.
- Key Elements for Strengthening State Laws and Policies Pertaining to Student Data Use, Privacy, and Security: Guidance for State Policymakers: EducationCounsel, a leading education law consulting firm, developed this document with guidance for state policymakers on the key foundational components to include in a privacy policy as well as model legislative language.
- The US Department of Education created the Privacy Technical Assistance Center (PTAC) as a resource on privacy, confidentiality, and security practices related to the use of student data. Among PTAC's many resources is Protecting Student Privacy While Using Online Educational Services, which clarifies when and how FERPA applies to student data collected by internet-based services. Another resource explains all of the FERPA exceptions.
- CoSN Protecting Student Privacy in Connected Learning Toolkit: This toolkit prepared by the Consortium for School Networking (CoSN) is a practical guide for school and district leaders on selecting and contracting with third-party service providers for data storage and management.

These recommendations were developed in collaboration with the following group of experts.

- Kathy Gosa, formerly of the Kansas Department of Education
- Chandra Haislet, Maryland Department of Education
- Daria Hall, The Education Trust
- Hans L'Orange, State Higher Education Executive Officers Association
- Rodney Petersen, EDUCAUSE
- Jay Pfeiffer, Consultant
- Maureen Wentworth, Council of Chief State School Officers
- Steven Winnick, EducationCounsel
- Kathleen Styles, US Department of Education (Advisory member)