EducationCounsel LLC

Key Elements for Strengthening State Laws and Policies Pertaining to Student Data Use, Privacy, and Security: Guidance for State Policymakers

Educators, students, parents, and policymakers need sound, actionable data to make informed decisions about improving student educational opportunities and outcomes. Among other practices and innovations, data help educators personalize learning and create dynamic, engaging classrooms; empower parents and the public to hold schools accountable for performance; and help ensure states and school districts purpose tax dollars toward effective programs and services. Given data's promise for improving teaching and learning, state policymakers must ensure that effective systems exist to nurture and support these important education data uses and other data-informed strategies for promoting students' college, career, and civic readiness.

At the same time, states and districts must make certain that data's incredible educational value is complemented by powerful safeguards that ensure the privacy and security of individuals' personally identifiable information (PII). Protecting students' privacy and information security is an important goal, which must be taken seriously by state leaders, administrators, educators, and other education data caretakers. These stakeholders must address very valid public concerns about inappropriate access to, or use of, student-specific data; the potential permanence of sensitive, personal information; and other related data privacy and security issues.

State policy can thoughtfully address these important challenges by harmonizing the educational advantages associated with effective data use with strong privacy protections for personally identifiable data across the education continuum (P-20) and into the workforce (P-20W). In an effort to assist states with developing policies reflecting the modern era of digitized education data, this guidance examines key issues and elements for state leaders to consider for protecting privacy and security of personally identifiable education and linked workforce data. Drawing from federal law, state examples, and an examination of best practices, this guide approaches education data privacy and security as comprehensively as possible.

Recognizing the state-specific context of these policy decisions, this guidance avoids recommending one-size-fits-all solutions or models. Privacy and security policy choices should be tailored to each state's unique context and needs. Ultimately, well-crafted state privacy policies must also be supported by adequate investment and training, and provide state educational agencies, districts, and schools with the ability to carry out their educational functions in innovative and effective ways. Given the complex and rapidly evolving education technology landscape, this document may be refined over time to reflect practical realities.

Foundational Elements of a State Data Privacy and Security Policy

In their quest to establish robust, actionable data systems that address today's educational needs, as well as prepare for unknown future needs, state policymakers should develop strong and comprehensive policies governing education data collection, storage, sharing, and analysis to ensure appropriate, effective safeguards for personally identifiable information. Many states already have undertaken or are in the process of this work, and their important efforts inform this guidance. Relevant federal laws, state practices, and emerging consensus regarding best practice demonstrate that state education data privacy and security policies include at least the following foundational components:

A. Statement of the **purposes of the state's privacy policies**, including an acknowledgment of the educational value of data and the importance of privacy and security safeguards;

B. Selection of a **state leader** and **advisory board** responsible for ensuring appropriate privacy and security protections, including for developing and implementing policies and for providing guidance and sharing best practices with schools and districts;

C. Establishment of a public **data inventory** and an understandable **description of the specific data elements** included in the inventory;

D. Strategies for promoting **transparency and public knowledge** about data use, storage, retention, destruction, and protections;

E. Development of **statewide policies for governing personally identifiable information;** and

F. Establishment of a **statewide data security plan** to address administrative, physical, and technical safeguards**.**

This guidance includes a brief background discussion of each component recommended above, along with a "State Legislation Checklist" in Appendix A (a table that links to the body of this guidance with recommended operational elements that should be considered for inclusion in state law or policy). These resources are coupled with "Model Legislative Language" in Appendix B, drawn from recent state examples, which provides ideas that may be useful when drafting relevant laws, regulations, or other policies.

Discussion and State Examples

As state leaders examine strategies for protecting personally identifiable education data, they should evaluate and consider the following recommendations and examples.

A. State the Purpose of the State's Privacy Policies

A state privacy policy should include a statement of purpose that acknowledges the educational value of effective data use and the paramount importance of establishing privacy and security safeguards to protect personally identifiable information. A purpose statement provides policymakers with an opportunity to express a clear commitment to education data privacy and a meaningful plan for achieving the state's privacy and information security vision. A well-designed purpose statement will also evidence state leaders' recognition of the importance of communicating effectively with students, parents, local education leaders, and other stakeholders with respect to these vitally important, but sometimes complex, issues. Lastly, a purpose statement establishes a guiding objective for the state and local leaders responsible for implementing the law.

For example, Idaho Senate Bill 1296 (2014) states:

> "It is the intent of the Legislature to help ensure that student information is safeguarded and that privacy is honored, respected and protected. The Legislature also acknowledges that student information is a vital resource for teachers and school staff in planning responsive education programs and services, scheduling students into appropriate classes and completing reports for educational agencies. Student information is critical in helping educators assist students in successfully graduating from high school and being ready to enter the workforce or postsecondary education. In emergencies, certain information should be readily available to school officials to assist students and their families. A limited amount of this information makes up a student's permanent record or transcript. The Legislature firmly believes that while student information is important for educational purposes, it is also critically important to ensure that student information is protected, safeguarded and kept private and used only by appropriate educational authorities and then, only to serve the best interests of the student. To that end, this act will help ensure that student information is protected and expectations of privacy are honored."

B. Create a Chief Privacy Officer or Equivalent Leader

States should create the role of a Chief Privacy Officer responsible for developing and overseeing the implementation of the state's education data privacy and security policies. Designating a well-qualified student privacy leader, and supporting their work by establishing an experienced advisory board, will demonstrate the state's commitment to protecting personally identifiable information and help ensure a strong and coordinated system of protections statewide.

The state's Chief Privacy Officer could be tasked, for example, with creating a public data inventory; developing best practices for school districts and schools; providing technical assistance, including disseminating best practices to all districts, schools, and other holders of covered data; leading oversight and accountability of the state's education data privacy framework (while honoring the need for local tailoring), and more. Depending on its needs and context, a state may find it best to vest responsibility for the state's privacy plan in: (1) an existing position, within an existing state agency or body; (2) a newly created position within an existing agency or body; or (3) a position in an entirely new agency or body.

State Examples: Vesting Responsibility for Privacy and Security Safeguards

Alabama's Board of Education created the position of Chief Privacy Officer, a first-in-the-nation position at the state level for education.

Oklahoma placed responsibility for carrying out the functions of its privacy and security law governing its statewide longitudinal data system in the state board of education.

Several states, including **Arizona, New York, Tennessee, and West Virginia** have introduced bills that would create the position of a Chief Privacy Officer within the state educational agency.

Maryland established an independent unit within state government to oversee data linked across agencies. The Longitudinal Data System Center has rulemaking authority. An authorized representative of the state department of education and the higher education commission, the Center's actual placement will be determined by its governing board.

As discussed below, in order to ensure comprehensive protections, the law should cover P-20W personally identifiable data, which will require effective privacy leadership and governance. Using a P-20W approach likely will involve multiple agencies and leaders, which state policymakers should consider as they work to identify an appropriate privacy leader for their unique context. Ultimately, all state agencies involved in the collection and use of P-20W data will need to support, and participate in, the development and execution of relevant laws and state policies. Coordination necessitates that there are responsible actors in leadership positions identified at each participating agency. For example, the executive governing body for Alaska's P-20W Statewide Longitudinal Data System (early childhood through the workforce statewide longitudinal data system) is composed of the Commissioner of the Alaska Department of Education and Early Development, the Commissioner of the Alaska Department of Labor and Workforce Development, the President of the University of Alaska, and the Executive Director of the Alaska Commission on Postsecondary Education. Regardless of his or

her location within state government, the privacy leader should be of sufficient seniority to ensure these important issues receive appropriate attention across the state's educational and workforce systems.

State leaders should ensure selection of the designated state privacy leader based on data privacy experience, qualifications, and education data expertise. Data privacy and security oversight requires familiarity with federal and state privacy laws and regulations, including the Family Educational Rights and Privacy Act ("FERPA"), Protection of Pupil Rights Amendment, Children's Internet Protection Act, Children's Online Privacy Protection Act, and corresponding state laws. Supervision of data systems also warrants technical sophistication and expertise in information security. For example, Maryland law requires that at least one public member of the Maryland Longitudinal Data System Center has expertise in large data systems and data security. Although a more narrowly targeted example, this idea could be applied to the broader position described by this section.

States also should establish a data oversight group with representatives of key state and local agencies, and possibly including one or more representatives of the governor and of parents and students. Such a board might be vested with policy-making authority or with an advisory role to help shape key data policies and oversee implementation.

C. Create a Data Inventory and Clearly Describe the Data Elements for the Public

State leaders should establish a data inventory that describes the types of personally identifiable education and workforce data collected and a description of the data's educational purposes. States should also consider describing (in lay terms) the data elements in the inventory in order to promote greater public understanding of data systems. States should also reflect on whether the inventory should include other information, such as the statutory or regulatory authority for a particular data collection. The inventory should be easily accessible to the public and be presented in a user-friendly format. No personally identifiable information should be available in connection with this public inventory.

A blended approach to inventorying and describing the data categories may work best. For example, state policy might establish the inventory, but empower the state's designated privacy leader to update the information and provide additional detail as necessary to promote greater public awareness and understanding about education data collection and use. States also may choose to include data elements regarding educators in the inventory, if performance data associated with evaluation systems is included in state or local data systems.

The following table illustrates how three states have described or proposed to describe certain education data.

State Data Privacy and Security Bills and Statutes that Inventory Covered Data		
	Student Data	**Other Defined Data**
Kentucky	**Education data** means the following data related to student performance from early childhood programs through postsecondary education: college and career readiness; course and grade; degree, diploma, or credential attainment; demographics; educator; enrollment; financial aid; high school equivalency diploma; remediation; retention; state and national assessments; transcripts; vocational and technical education information; and any other data impacting education deemed necessary by the Office for Education and Workforce Statistics.	**Workforce data** means data relating to certification and licensure; employer information; employment status; geographic location of employment; job service and training information to support enhanced employment opportunities; wage information; and any other data impacting the workforce deemed necessary by the Office for Education & Workforce Statistics.
Maryland	**Student data** means data relating to student performance. Student data includes state and national assessments; course-taking and completion; grade point average; remediation; retention; degree, diploma, or credential attainment; enrollment; and demographic data. Student data does not include juvenile delinquency records, criminal and CINA records, medical and health records, and discipline records.	**Workforce data** means data relating to employment status, wage information, geographic location of employment, and employer information.
Tennessee	**Student data** means data collected and/or reported at the individual student level included in a student's educational record. Student data includes state and national assessment results, including information on untested public school students; course taking and completion, credits earned, and other transcript information; course grades and grade point average; date of and drop-out data; attendance and mobility; data required to calculate the federal four-year adjusted cohort graduation rate, including sufficient exit and drop-out information; discipline reports limited to objective information sufficient to produce the federal Title IV Annual Incident Report; remediation; special education data; and demographic data and program participation information. Unless included in a student's educational record, student data shall not include juvenile delinquency records, criminal records, medical and health records, student Social Security number, and student biometric information.	**Teacher data** means personal summative and evaluation scores, the access to which is limited to district administrators, local boards of education, or those with direct supervisory authority who require such access to perform their assigned duties.
Sources: KY. REV. STAT. Ch. 151B (2013); MD. CODE ANN., Maryland Longitudinal Data System, § 24-701 *et seq.* (2010); Tennessee S.B. 1470 (2014).		

States also should consider whether the data inventory should expressly acknowledge the multiple formats in which personally identifiable student information may exist. For example, PII may be found in physical or digital documents, images, videos, and other files.

D. Establish Policies to Promote Greater Public Transparency about Data Use

State leaders should examine other strategies for promoting public understanding and awareness of state, district, and school education data practices and strategies for protecting PII. For example, state policy might encourage or require state and district leaders to provide, annually or on another routine basis, information to students, parents, and other stakeholders about state and related local privacy policies, activities, and other important developments. States might develop policies that provide advance notice about significant new state and local data initiatives and practices. States also should consider establishing formal and accessible pathways for parents and the public to ask questions and seek additional information about data use practices and protections.

States should be clear and transparent about how data are used by state education personnel, contracted vendors, and researchers. The state should specify what data are sent to the federal government, providing references to the legal authority allowing this sharing of data and specify what is kept at the state level. The state should publicly state the retention policies for student data and the process and timelines for destruction of PII.

E. Establish Statewide Protections for Personally Identifiable Information

States should develop and adopt robust education data privacy policies that complement FERPA to guide state and local efforts to protect personally identifiable information. Establishing a statewide system designed to protect PII will promote consistency and fidelity to privacy best practice among all covered institutions and agencies. Specifically, state policymakers should consider addressing the following privacy and security issues:

1. *Authorized access to personally identifiable information.* State policy should address the circumstances when a public employee or contractor may access personally identifiable information, consistent with FERPA and state law. Only persons with a legitimate need for the data to support their professional roles should have access to PII. These policies should recognize varied local situations and evolving circumstances and therefore provide local school districts with sufficient flexibility to tailor solutions. See, for example, Maryland law, MD. CODE ANN., Maryland Longitudinal Data System, § 24-701 *et seq.* (2010).

2. *Approval criteria for data-sharing requests*. Requests for personally identifiable student data, including for research or audits and evaluation, should be judged based on published criteria. Consistent with FERPA regulations, states should provide legal authority for the state actor to enter into agreements with third parties for studies to improve instruction or develop assessments and provide student data for that purpose on behalf of school districts or schools from which the data were

obtained. Established criteria also can govern access to student data in connection with an audit or evaluation of a federal- or state-supported program. State policy should ensure that any public report resulting from the data obtained via such research or evaluation requests include only aggregate, non-personally identifiable data.

3. *Creation of a detailed data security plan*. Privacy policies should include a security plan to govern use and maintenance of data systems with attention to ensuring the use of appropriate administrative, physical, and technical safeguards. Necessary components of such a plan are discussed below, in Element F. See also Massachusetts's regulations imposing minimum security requirements, 201 Mass. Code Reg. 17.00.

4. *Notifications to parents and students*. States should establish policies designed to notify parents and students about their privacy rights under federal and state law. For example, under FERPA regulations, parents and students who are at least 18-years-old or enrolled in postsecondary education have the right to inspect and challenge the accuracy of content in their student education records.

5. *Prohibit use of data for non-educational purposes.* Consistent with FERPA, state policy should prohibit the use of data for non-educational purposes, including the sale of data or its use for marketing purposes (except with regard to authorized uses of directory information not obtained through a contract with an educational agency or institution). The U.S. Department of Education's recent guidance, *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices*, is a useful resource to consult when developing policies to effectuate these protections.

6. *Consequences for the misuse of data.* State policy should establish consequences or require the state actor to establish consequences for state employees and employees of contractors that intentionally, recklessly, or negligently fail to comply with established policies regarding data privacy and security. For example, FERPA regulations provide for a five-year disbarment of any third-party that violates provisions governing access to student PII. The state law may establish similar, or more stringent, terms, including employment sanctions for individual employees such as reprimands, suspensions, and termination of employment. In assessing appropriate consequences, state policymakers should consider whether gross negligence, at a minimum, should be established and whether a modicum of harm needs to be shown. See, for example, Oklahoma law, OKLA. STAT. tit. 70, § 70-3-168 (2013).

7. *Apply Data Privacy and Security Policies to Contractors and Vendors.* States, districts, and schools have long relied on the expertise of contractors and vendors – both for-profit and nonprofit - in carrying out their mission of providing quality education to students. While mindful of the great value of these partnerships, state

policy should definitively extend data privacy and security requirements to contractors and vendors. Working with the state's Chief Privacy Officer or equivalent, state agencies and districts should craft contracts with vendors to specify certain safeguards, including allowing audits of vendor security risk assessments, restricting use and reuse of data collected, and destroying data upon termination of the contract. See, for example, Tennessee legislation, S.B. 1470 (2014)

8. *Invest in training and other supports to build state and district capacity.* Providing robust privacy protections for PII requires not only strong policies, but also resources to help state agencies, school districts, schools, and other stakeholders successfully implement the policies. This includes significant investments in technical assistance, professional development, and planning.

F. Require a Data Security Plan

State and local education and related workforce PII should be protected by a security plan that addresses necessary administrative, physical, and technical safeguards. Such a security plan should: (1) establish minimum **data privacy and security compliance standards**; (2) require **regular privacy and security compliance audits**; (3) require **breach notification and mitigation procedures;** and (4) identify **storage and security protocols**, including data retention and destruction policies. Safeguards that should be considered for inclusion in the data security plan include, but are not limited to, the following:

Security Protocols	Options
Administrative	• Authorization and authentication mechanisms for accessing PII • Monitoring of system, including data requests and disclosures, access logs, security incident tracking reports, and periodic access audits • Sanctions for employees and contractor personnel who fail to comply with security policies and procedures • Processes to continually identify threats to data security and to address those threats • Background checks for permanent and temporary employees, vendors, and contractors, at the state, regional, and local levels before they receive access to PII • Policies for masking data from small groups ("small cell size data") • Policies and processes for destruction of data when no longer needed and for verifying such destruction
Physical	• Security awareness through training and other guidance • Incident response plan for documenting and responding to suspected or known security incidents. • Limited physical access to PII and facilities in which PII are stored • Storage of PII in approved secure repositories, rather than on shared or local drives

Security Protocols	Options
	• Appropriate limitations on downloading PII to local or portable devices • Procedures that govern the movement of hardware and electronic media that contain PII
Technical	• Safeguards, including data encryption, to ensure PII transmitted over communications networks is not accessed by unauthorized person or groups • Procedures that protect PII from improper alteration or destruction • Automatic log-offs for inactive users

Conclusion

Education data use and new technologies hold incredible promise for improving the educational experiences and outcomes of students. At the same time, personally identifiable information demands highly effective privacy and security safeguards. This is increasingly imperative as data are digitized and accessed and used via new technologies. The materials that follow in Appendices include: (A) a checklist for states to consult as they craft laws and corresponding policies; and (B) an example of legislative language that can serve as a model for state policymakers grappling with these issues.

State leaders may pursue different, equally reasonable options on particular issues, in light of each state's unique context. Issues of privacy and security will evolve over time as new technologies and capabilities emerge; given this changing landscape, this document will be updated as warranted. Ultimately, state laws should establish a policy framework that acknowledges and communicates the value of data to teaching, learning, and decision-making while ensuring that effective privacy, security, and confidentiality safeguards are in place to protect the private information of students.

EDUCATIONCOUNSEL, LLC and NELSON, MULLINS, RILEY AND SCARBOROUGH LLP

For further information, please contact a member of the EducationCounsel and Nelson Mullins education data privacy and security team: **Reg Leichty, Partner**, **David Katz, Partner, Art Coleman, Managing Partner**, **Steve Winnick, Senior Counsel and Kate Lipper, Policy and Legal Advisor.**

www.EducationCounsel.com

www.NelsonMullins.com

Appendix A
State Legislation/Policy Checklist
for Student Data Use, Privacy, and Security Laws

The following table synthesizes the guidance and recommendations provided in *Key Elements for Strengthening State Laws and Policies Pertaining to P-20W Student Data Use, Privacy, and Security: Guidance for State Policymakers* by itemizing the components within each element of a comprehensive student data use, privacy, and security policy set. State policymakers can compare draft legislative or other policy language against this checklist to determine whether their language appropriately and effectively addresses the suggested elements.[1] Recognizing that each state has a unique legal and educational context, these issues may warrant or even require different approaches in different states, including through the use of law, regulation or other policy depending on a specific state preference and legal framework.

Elements are color-coded to assist policymakers with cross-references to the Model Legislative Language provided in Appendix B.

State Student Data Use, Privacy, and Security Legislation Checklist	
Key Element	**Status**
A. State the Purpose of the State's Privacy Law	
☐ The legislation states the purpose, or intent, of the measure.	
B. Designate a State Leader for Protecting Education Data	
☐ **B1)** The legislation identifies the state leader responsible for protecting personally identifiable education data and overseeing implementation of this law.	
☐ **B2)** The legislation states whether the responsible state leader has rulemaking or policy-making authority or serves in an advisory or enforcement role.	
☐ **B3)** The legislation is clear on the scope of the state leader's authority.	
☐ **B4)** The legislation establishes an education data oversight board, and ensures that responsible actors at each participating state agency assist collaborate and ensure consistency in data privacy and security practices.	
☐ **B5)** The legislation identifies, or requires an appropriate state leader to identify, necessary qualifications or compositional requirements for the state privacy leader.	
C. Create a Data Inventory and Clearly Describe the Data Elements	
☐ **C1)** The legislation provides for the creation of a public data inventory that offers a complete list of the data elements collected by the state, or the statewide longitudinal data system **[SLDS]**, and the rationale for collecting those elements.	
o (Optional Additional Detail) *The legislation includes other requirements for the inventory such as the statutory or regulatory authority for a particular collection,*	

[1] While the checklist refers to state legislation or law, the checklist also can be used in developing state policy through other means such as regulations or policy guidelines.

State Student Data Use, Privacy, and Security Legislation Checklist	
Key Element	**Status**
data elements that have been proposed for inclusion, information on the purposes and uses of the data, etc.	
☐ **C2)** The legislation identifies the location of the public data inventory (e.g., the state educational agency website) or requires the responsible state actor to house the inventory in an accessible, prominent location.	
☐ **C3)** The legislation covers P-20 education data.	
☐ **C4)** The legislation covers use of workforce data for educational purposes.	
☐ **C5)** (Optional Additional Detail) *The legislation covers educator or teacher data.*	
☐ **C6)** The legislation ensures that school districts, schools, and public early childhood programs also will provide comparable public information regarding the personally identifiable information **[PII]** that they collect.	
D. Establish Policies to Promote Greater Public Transparency about Data Use	
☐ **D1)** The legislation tasks the responsible state actor with developing policies for providing information to parents and the public on: (1) proposed significant data initiatives, their purposes, and how the data will be used; (2) opportunities for parents and the public to raise concerns and issues regarding such initiatives; and (3) data privacy and security protections.	
☐ **D2)** The legislation ensures that school districts, schools, and public early childhood programs also will provide comparable public information.	
E. Identify Necessary Statewide Policies for Personally Identifiable Information	
☐ **E1)** The legislation directs the responsible state actor to adopt policies regarding employee and contractor access to PII.	
☐ **E2)** The legislation authorizes the responsible state actor to enter into agreements with third parties (a) for studies to improve instruction or develop assessments and (b) to audit or evaluate a federal- or state-supported program, and to provide student data for those purposes on behalf of the school districts or schools from which the data were obtained.	
o **E2a)** The legislation directs the responsible state actor to develop approval criteria for data-sharing requests, including for research or evaluations.	
o **E2b)** The legislation establishes that any public report resulting from data obtained via such requests only include aggregate, non-personally identifiable information. [already required by the Family Educational Rights and Privacy Act]	
o **E2c)** The legislation establishes that PII shall not be provided to the federal government except where compelled by a court order or subpoena or otherwise required by law.	
☐ **E3)** The legislation directs the responsible state actor to design and implement a data security plan [**see Element F**] to govern use and maintenance of the SLDS and other state data systems, including for all agencies that provide data to the SLDS and other state data systems.	
☐ **E4)** The legislation requires that the state actor develop a policy for notifying parents and students of their legal rights under federal and state law with respect to data use, privacy, and security.	

State Student Data Use, Privacy, and Security Legislation Checklist	
Key Element	**Status**
☐ **E5)** (Optional Additional Detail) *The legislation enumerates other necessary statewide policies that the responsible state actor must develop and implement.*	
☐ **E6)** The legislation empowers the state actor to develop additional policies necessary to implement the law and to monitor and investigate compliance with the regulations/policies developed to implement this law.	
☐ **E7)** The legislation establishes consequences for noncompliance with privacy and security policies by individual employees and contractors.	
☐ **E8)** The legislation ensures that school districts, schools, and public early childhood programs have comparable policies for their data systems.	
F. Require a Data Security Plan	
☐ **F1)** The legislation requires that the data security plan developed by the responsible state actor has **administrative** safeguards.	
o (Optional Additional Detail): *The legislation expressly identifies certain administrative safeguards, or requires that certain administrative safeguards be addressed in the plan, such as authorization and authentication mechanisms; monitoring of system; sanctions for noncompliance; and processes to identify threats.*	
☐ **F2)** The legislation requires that the data security plan developed by the responsible state actor has **physical** safeguards.	
o (Optional Additional Detail) *The legislation expressly identifies certain physical safeguards, or requires that certain physical safeguards be addressed in the plan, such as security awareness training and guidance; incident response plan; limited physical access; procedures for movement of hardware and electronic media; and data encryption.*	
☐ **F3)** The legislation requires that the data security plan developed by the responsible state actor has **technical** safeguards.	
o (Optional Additional Detail) *The legislation expressly identifies certain technical safeguards, or requires that certain technical safeguards be addressed in the plan, such as encryption, procedures to protect against improper alteration or destruction, and automatic log-offs for inactive users.*	
☐ **F4)** The legislation requires regular compliance audits of the SLDS and other state data systems.	
☐ **F5)** The legislation requires breach notification and mitigation procedures.	
☐ **F6)** The legislation provides for the development of storage and security protocols, including data retention and destruction policies.	
☐ **F7)** The legislation requires background checks, training, and privacy and security agreements for employees at the state and local levels before they receive access to PII.	
☐ **F8)** The legislation directs the responsible state actor to develop model data privacy and security policies and complementary training resources that local agencies, including school districts, can adopt and use.	
☐ **F9)** The legislation ensures that data security policies exist for all state and local agencies that collect and maintain student PII.	

State Student Data Use, Privacy, and Security Legislation Checklist	
Key Element	**Status**
G. Apply Data Privacy and Security Policies to Contractors and Vendors	
☐ **G1)** The legislation extends the data privacy and security requirements to contractors and vendors of the state.	
☐ **G2)** The legislation extends the data privacy and security requirements to contractors and vendors of school districts, schools, and other educational agencies and institutions in the state.	
☐ **G3)** (Optional Additional Detail) *The legislation establishes penalties for contractors that fail to comply with privacy and security precautions and provisions.*	

Appendix B
Model Legislative Language
Student Data Use, Privacy, and Security Law

This document provides model legislative language to state policymakers considering legislation on the use and protection of student data. Given diverse state educational authorities and government organizational structures, this example text should be reviewed as a starting point, and individual states may choose to approach these matters differently. For example, this bill places responsibility for the implementation of the law with state educational agency entities, but other bills might approach this issue differently. Likewise, this bill establishes a Chief Privacy Officer with the authority to develop regulations and policies that govern the data systems of all educational agencies and institutions in the state, from preschool through graduate school, as well as workforce data; this approach may not work in certain states, given their legal frameworks. Using the language that follows below as a resource, policymakers can modify and refine these provisions to meet their state's needs. Elements are color-coded to assist policymakers with cross-references to the Policy Checklist provided in Appendix A.

----------♦----------

Title: Student Data Use, Privacy, and Security Act

Section 1. **[A]** Legislative Findings and Purpose.

(a) *Findings.* (1) Student information is a critical tool for educators in order to plan and provide education programs and services that are responsive to student needs and ensure that the State's education system prepares students effectively for college, career, and citizenship.

(2) While it is critical that educators be able to use student information for educational purposes, it is also vitally important that student information is protected, safeguarded, and kept private and used only by appropriate educational authorities in order to serve the best interests of students.

(b) *Purpose.* The purpose of this act is to help ensure the privacy and protection of student information by adopting policies for the appropriate use of student data and for the development and implementation of appropriate privacy and security safeguards governing that use.

Section 2. State Data.

The state educational agency is authorized to use data –

(a) To evaluate public education programs at all levels, from preschool through postsecondary graduate school;

(b) To conduct and support research studies designed to improve instruction or to develop assessments for or on behalf of schools or school districts in the state; and

(c) To provide services to school districts, schools, and preschool programs throughout the state.

Section 3. **[B]** Administration.

(a) *General*. This act shall be administered by a Chief Privacy Officer appointed within the state educational agency and subject to oversight and approval of actions by the State Data Oversight Board, as specified in this act.

(b) **[B4]** *State Data Oversight Board.* The State Oversight Board shall include representatives of the Governor, the state educational agency, the state department of workforce development, the state department of postsecondary education, [state colleges], local school districts, preschool agencies, and parents and students in the state. [**[B5]** address composition and size of Board, including whether appointments are made by state leaders, including Governor]

(c) **[B1, B3]** *Chief Privacy Officer.*

(1) A Chief Privacy Officer with experience in developing and implementing data privacy and security policies shall be appointed by the Chief State School Officer in consultation with the State Data Oversight Board.
(2) The Chief Privacy Officer shall report directly to the Chief State School Officer and shall be subject to the oversight and approval functions vested by this act in the State Data Oversight Board.
(3) With the approval of the State Data Oversight Board, the Chief Privacy Officer shall –
    (i) Develop data privacy and security **[B2]** [regulations/policies] – including policies regarding the transparency of data system policies, processes, and initiatives – for data maintained by the state and for the data systems of school districts, schools, and other public educational agencies or institutions in the state;
    (ii) Supervise, monitor, and investigate implementation of such [regulations/policies] by the state and by school districts, schools, and other public educational agencies and institutions;
    (iii) Develop and provide a program of training and technical assistance, including the dissemination of best practices, to school districts, schools,

and other public educational agencies and institutions in the implementation of such [regulations/policies];

(iv) Develop and provide a program of accountability, governance, oversight, and audit to be executed by the state and individual school districts, schools, and other public educational agencies and institutions in order to implement such [regulations/policies], including policies for the designation of responsible officials in each agency or institution for implementing policies adopted pursuant to this act and for coordinating with the state educational agency; and

(v) Develop recommendations – for submittal to the Legislature through the Chief State School Officer – for necessary funding to implement this act, including investments in building the capacity of the state and other public educational agencies and institutions effectively to meet their obligations under this act.

Section 4. **[C]** State Data.

(a) *Sources of data.* As determined to be necessary by the Chief Privacy Officer, and in accordance with applicable state and federal law, personally identifiable student and educator data shall be provided to the state educational agency by local school districts; public schools; pubic preschool programs; the state postsecondary agency; public postsecondary institutions in the state; and the state workforce agency, which shall also provide workforce data to the state educational agency.

(b) **[C1]** *Data Inventory.* (1) The Chief Privacy Officer, with the approval of the State Data Oversight Board, shall develop, regularly update, and make available to the public **[C2]** on the state educational agency website and through such additional methods as may facilitate accessibility an inventory and an understandable description of the personally identifiable data to be maintained by the state, including—

(i) **[C3]** Data relating to student performance, including data on state, local, and national assessments; course-taking and completion; grade-point average; remediation; retention; degree, diploma, or credential attainment; enrollment; and demographic data;

(ii) **[C4]** Workforce data, including employment status, wage information, field of employment, employer information, and geographic location of employment;

(iii) **[C5]** Teacher data, including teacher evaluations and demographic data and performance data for the students taught, with access to such data limited to local school boards or those with direct supervisory authority who have a legitimate need for such information to assess teachers, participate in making equitable assignments of effective teachers, or develop and implement supports for teachers; and

(iv) Other student and workforce data deemed necessary by the State Data Oversight Board to achieve the state's educational goals.

(2) As determined by the Chief Privacy Officer, with the approval of the State Data Oversight Board, the data inventory shall include information on the statutory or regulatory authority for collecting and maintaining the data; the purposes of doing so; and the intended uses and disclosures of the data.

Section 5. Definitions.

(a) "*Data*" includes student data from preschool programs through postsecondary graduate school programs that receive public funds and employee workforce information in whatever format, including documents, images, videos, and other files.

(b) *"Eligible student"* means a student who is at least 18-years-old or is enrolled in a postsecondary institution.

(c) "*Oversight Board*" means the State Data Oversight Board constituted in accordance with Section 3 of this act.

(d) *"Personally identifiable information"* means the student's name; the name of the student's parent or other family members; the address of the student or student's family; a personal identifier, such as the student's social security number, student number, or biometric record; other indirect identifiers such as the student's date of birth, place of birth, and mother's maiden name; other information that, alone or in combination, is linked or linkable to a specific student and enables a person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or information requested by a person who the educational agency or institution reasonably believes knows the student to whom the education record relates. It also includes parallel information related to teachers and members of the workforce. [This definition tracks U.S. Department of Education's FERPA regulations.]

(e) "*Preschool program*" means an early childhood education program, as defined in regulations under the Family Educational Rights and Privacy Act, 34 CFR 99.3.

Section 6. **[D]** Transparency

(a) *General.* The Chief Privacy Officer, with the approval of the Oversight Board, shall develop statewide [regulations/policies] regarding transparency **[D1]** for the state's data system[s] **[D2]** and for the data systems of school districts, schools, and other public educational agencies and institutions in the state.

(b) **[D1]** *Specific regulations/policies.* The regulations/policies shall address:

(1) Accessibility to parents, students, and the public of the data inventory described in section 4, including understandable and up-to-date information on the purposes, uses, and authorized disclosures of data maintained by the state;

(2) **[E4]** The rights of parents and students regarding their personally identifiable information under federal and state law;
(3) The opportunity of parents or students to receive advance notice of broad-scale data initiatives or disclosures – including proposals to outsource maintenance of data or significant functions and services requiring the use of personally identifiable data – and an opportunity to raise issues and comment thereon;
(4) Parent, student, and public access to clear and comprehensive information on data privacy and security safeguards to protect data from unauthorized release or use or from data breaches; and
(5) Processes and the provision of contact information for parents and students to raise issues or concerns regarding the collection and use of their personally identifiable data.

(c) *Annual report.*
(1) The Chief Privacy Officer shall prepare an annual report, which shall be reviewed prior to submission by the Oversight Board and the Chief State School Officer, for submission to the Governor and the State Legislature.
(2) The annual report, which shall be made public, shall –
(i) Report on the implementation of the provisions of this act;
(ii) List broad-based data initiatives begun or being planned, including significant research studies to be implemented with data provided by the state;
(iii) Identify significant threats to data privacy and security, including such threats in particular school districts, schools, or other participating agencies;
(iv) Report on the results of data system audits; and
(v) Include recommendations for significant improvements to the state data systems.

Section 7. **[E, F]** Data Privacy and Security Policies

(a) *General.* The Chief Privacy Officer, with the approval of the Oversight Board, shall develop statewide [regulations/policies] regarding data privacy and security – consistent with state and federal law, including the Family Educational Rights and Privacy Act, 20 U.S.C. 1232g, the Protection of Pupil Rights Amendment, 20 U.S.C. 1232h, the Children's Online Privacy Protection Act, 15 U.S.C. 6501, and the Children's Internet Protection Act, 47 U.S.C. 254 – for the state data system[s] and **[E8, F9]** for the data systems of the school districts, schools, and other public educational agencies and institutions in the state, including preschool programs.

(b) *Specific* [*regulations/policies*]. The [regulations/policies] shall address:
(1) Data privacy protections, including—
(i) **[E1]** Responsibility and processes for determining who has access to the data based on legitimate need, consistent with federal and state law;

(ii) Definitions of small cell size data that alone or in combination with other available data may be linkable to individuals, and policies for suppressing small cell size data;

(iii) **[E2, E2a]** Criteria for determining whether a proposed use of personally identifiable data or de-identified data for studies to improve instruction or to develop assessments are for the benefit of school districts, schools, or other public educational agencies and institutions such as preschool programs that enroll students in the state;

(iv) **[E2b]** Processes to ensure that only anonomyzed aggregate or de-identified data are used in public reports or other public documents, apart from directory information that is releasable to the public consistent with the Family Educational Rights and Privacy Act; and

(v) **[E2c]** Non-disclosure of personally identifiable information to Federal agencies, except where compelled by court order or subpoena or otherwise required by law, such as complying with civil rights data reporting obligations.

(2) **[E3, F]** Data security protections, in the form of a statewide data security plan, including— [the following are examples of protections that legislators should consider including in a bill, to be addressed by the Chief Privacy Officer]

(i) **[F1]** Authorization and authentication mechanisms for accessing personally identifiable information;

(ii) **[F1]** Data system monitoring, including access logs, intrusion prevention and detection systems, data loss prevention tools, penetration testing, security incident tracking reports, and periodic access audits;

(iii) **[E7, F1-2, 7]** Employee (including employees of contractors) processes, including background checks for employees who have access to personally identifiable data; employee written agreements to comply with data privacy and security policies; continuing security awareness training for employees; and sanctions for employees who do not comply.

(iv) **[F4]** Regular privacy and security compliance audits;

(v) **[F1-2, 5]** Processes for the continuing identification of and response to threats to data security;

(vi) **[F2-3]** Data encryption for all mobile computing devices, hardware, and data repositories containing personally identifiable data;

(vii) **[F2, 5]** Incident response plans for documenting and responding to suspected or known data security incidents, including breach notification and mitigation procedures;

(viii) **[F2]** Limited physical access to personally identifiable information and facilities in which it is stored;

(ix) **[F2]** Procedures that identify, track, monitor, and decommission all hardware and electronic media that contain personally identifiable information;

(x) **[F2-3]** Safeguards, including encryption, to ensure personally identifiable information transmitted over communications networks are not accessed by unauthorized persons;

(xi) **[F3]** Procedures that protect personally identifiable information from improper alteration or destruction;

(xii) **[F3]** Automatic log-offs for inactive users;

(xiii) **[F6]** Destruction of personally identifiable information when it is no longer needed for authorized educational purposes, including processes to ensure and document reliable destruction;

(xiv) **[F6]** Wiping of portable electronic devices such as laptops, tablets, and mobile phones when no longer utilized by school districts, schools, and other public educational agencies and institutions in the state, including preschool programs; and

(xv) Procedures that prescribe methods to sanitize all media containing personally identifiable information.

(3) **[E7]** Penalties, whether administrative, financial, or both, for employees and contractors of the state or of school districts, schools, or other public educational agencies and institutions in the state that violate the privacy and security policies and procedures established pursuant to this act, including possible suspensions and terminations of employment.

(c) **[G]** *Application to Third-Party Vendors and Contractors.*

(1) **[G1-2]** Data privacy and security regulations or policies developed pursuant to this statute shall apply to all third-party vendors and contractors that are given physical or electronic access to personally identifiable information in order to perform outsourced services for the state or for school districts, schools, and other public educational agencies or institutions in the state and shall be incorporated in the applicable contract documents.

(2) **[G1-2]** Third-party vendors and contractors that receive personally identifiable information from the state or from school districts, schools, or other public educational agencies or institutions in the state shall use the information solely to provide the contracted-for service.

(3) **[G1-2]** A proposed third-party vendor or contractor shall certify in writing in advance of the contract or in applicable contract documents that it shall comply with the regulations or policies issued pursuant to this law and that it will not unilaterally revise any contractual provisions relating to the use, privacy, and security of personally identifiable information provided to it.

(4) **[G1-2]** A third-party vendor or contractor that receives personally identifiable data shall not disclose data without the written permission of the state or other agency or institution from which it received the data or absent the express written consent of all parents (or eligible students or workers) whose records would be disclosed.

(5) **[G3]** Contracts subject to this section shall include enforcement sanctions for contractors that do not comply with these requirements.

(d) *Prohibition on data use for marketing.* Data maintained by the state, or by school districts, schools, or other educational agencies or institutions in the state, including data provided to contractors, shall not be sold or used for marketing purposes (except

with regard to authorized uses of directory information not obtained through a contract with an educational agency or institution).

(e) *Distinguishing state data systems and other data systems.* Nothing in this law shall prohibit the Chief Privacy Officer – in developing [regulations/policies] under this law – from prescribing more specific [regulations/policies] for the state data system[s] than it prescribes for school districts, schools, and other public educational agencies and institutions in the state and permitting such agencies and institutions to adopt their own, supplementary [regulations/policies] tailored to their own needs.

Section 8. **[E2]** Authority for Research Studies

The state educational agency is authorized to enter agreements for studies to improve instruction or develop assessments and disclose personally identifiable information or de-identified data needed for such studies to the appropriate research organization on behalf of school districts, and schools, and other public educational agencies and institutions in the state, subject to contracts with the research organization that comply with the Family Educational Rights and Privacy Act and the requirements of this act.

Section 9. **[F8]** Training and Technical Assistance.

The Chief Privacy Officer shall develop and ensure the provision of training and technical assistance to local school districts, schools, other educational agencies and institutions, and state agencies that maintain student, workforce, or educator data to ensure understanding of the regulations/policies issued under this act; to assist in the development of supplementary data privacy and security policies, as needed; and to build a culture of privacy and security across the state educational agency and other public participating agencies in the state and transparency to the public.

Section 10. Severability clause.

The provisions of this act are severable. If any part of this act is declared invalid or unconstitutional, that declaration shall not affect the part or parts that remain.

Section 11. Effective date.

This act shall become effective [date].