



## OPERATIONAL PLAN

# Student Data Protection Office

Alija Blackwell

The New Mexico Public Education Department (NMPED) should establish a state Student Data Protection Office (SDPO) that would enforce student data protection agreements in the edtech vendor procurement process and lead collective capacity building efforts to support students, caregivers, education personnel, and school partners. This document provides further details as to how NMPED should build and structure this office.

## Creating a Student Data Protection office

The proposed student data protection agreement would require annual training, ongoing monitoring, and implementation overseen by a Student Data Protection Office. The US Department of Education's Elementary and Secondary School Emergency Relief (ESSER) Fund would pay for this initiative, as ESSER funding is supposed to be used to "promote long-term improvements in technology infrastructure and operations and their effective use."<sup>1</sup> This investment would ensure that New Mexico creates the foundational infrastructure for future-ready schools.

The New Mexico Public Education Department (NMPED) should operationalize the Student Data Protection Office by proceeding in 5 steps:

1. Staff the office with a state chief student data steward, Local Education Agency (LEA) and Tribal Education Department (TED) data lead, and TED/LEA information security steward;
2. Create a data sovereignty plan template for each TED/LEA;

3. Provide statewide trainings to the office and school district personnel alongside school communities interfacing with student data;
4. Engage an interdisciplinary Student Data Protection Advisory Council of youth, caregivers, and teachers; and
5. Collaboratively design the Student Data Protection Office strategic vision.

### **1. STAFF**

NMPED should hire a state chief student data steward to facilitate the hiring, management, and training of TED/LEA data leads and TED/LEA information security stewards. See the job descriptions in the Appendix to learn more about how the state chief student data steward, TED/LEA data lead, and TED/LEA information security steward would contribute to comprehensive student data protections statewide.

### **2. DATA SOVEREIGNTY PLAN**

Each TED/LEA data lead and information security steward should establish a [data sovereignty plan](#) with the Tribal Education Departments and school districts. The plan should focus on providing a series of policies and responsibilities about retaining and restoring data ownership rights to the communities where the data are collected. To create future-ready schools, the NMPED's Student Data Protection Office also should ensure that students, parents, and caregivers are equipped with the necessary tools and information to exercise their digital rights. See the Data Sovereignty Plan Template to learn more about key elements to include in this document to guide the TEDs/LEAs in establishing data protection and security protocols that foster data agency with students, parents, caregivers, and school personnel.

### **3. TRAININGS AND COLLECTIVE CAPACITY BUILDING**

The state chief student data steward, TED/LEA data leads, and TED/LEA information security stewards will be responsible for training and supporting educators and staff regarding federal and state data privacy laws to ensure legal compliance. The Student Data Protection Office would also

facilitate capacity building efforts across students, parents, caregivers, and school partners. See [Capacity Building Materials](#) for schools that include personnel trainings, student digital rights class materials, and parent and caregiver capacity building materials to learn more.

#### **4. STUDENT DATA PROTECTION ADVISORY COUNCIL**

The Student Data Protection Office should collaborate with the NMPED's Student Leader Network, Teacher Leader Network, Family Cabinet, Civic Leader Network, and the Secretary's Family Cabinet Advisory to create a Student Data Protection Advisory Council.<sup>2</sup> The council would contribute to the NMPED's ongoing platforms for community engagement and trust building to ensure voice equity in policy decisions related to education data protection, procurement, and the strategic vision for the Student Data Protection Office with parents, caregivers, students, civic leaders, and teachers.<sup>3</sup> The Student Data Protection Advisory Council should reflect the diverse school communities served.

#### **5. STUDENT DATA PROTECTION OFFICE STRATEGIC VISION**

Finally, the Student Data Protection Office should establish a strategic vision with the guidance of the advisory council and colleagues across the NMPED and Tribal Education Departments. It should encompass three key elements: (A) collective capacity building for digital literacy, (B) cradle to career data protection; and (C) data sovereignty.

##### **A. Collective Capacity Building for Digital Literacy and Data Agency**

As the state Department of Information Technology and NMPED work toward expanding broadband access and making historic investments in education technology infrastructure, it is critical to simultaneously engage in a multiyear capacity building effort to ensure digital literacy of key stakeholders across sectors. This collective effort should entail professional development trainings, workshops and seminars for school community members, and learning interventions to foster a greater sense of data agency. By investing in the frontline stakeholders, the state can take proactive measures to ensure that with increased broadband access comes increased understanding of how to safely navigate digital environments.

##### **B. Cradle to Career Data Protection**

Given the nature of data profiling and data repurposing across third parties, it is necessary to implement comprehensive data protection practices and secure the technology infrastructure across lifelong learners' academic and professional careers. As New Mexico's Early Childhood [Education &](#)

Care Department plans to create a statewide integrated data system, the Student Data Protection Office should ensure student data protection by design.<sup>4</sup> The office should evaluate points of intervention across departments and systems to ensure that necessary protections are in place as student data travel across public and private sector systems.

### C. Data Sovereignty

The office should establish coordinated pathways for students, teachers, and parents or caregivers to determine how to share their data, the purpose for the use of their data, and the conditions of the storage and protection of data. Through exploring blockchain for education data sharing, dynamic consent mechanisms, and self-sovereign identity tools, the office should design platforms for school communities to exercise their digital rights. These rights should include the ability to access, amend, delete, and interpret data, and to opt out of data collection. The office should also ensure data sovereignty protocols with tribal education leaders through the Tribal Education Departments and Native Procurement Technical Assistance Centers. Students and caregivers should have transparent opportunities to seek recourse and accountability for any violations to their data sovereignty.

*For further details on these recommendations, please refer to the [attached Student Data Protection Office policy brief](#), [student data protection agreement template](#), and [materials for schools to implement the student data protection agreement once established](#), including a [TED/LEA data sovereignty plan template](#) and [capacity building materials for students, educators, parents, and caregivers](#).*

## Appendix

### **NMPED CHIEF STUDENT DATA STEWARD JOB DESCRIPTION**

The chief student data steward will establish and enforce statewide systems for ensuring that school districts comply with student data protection laws and regulations and are building the capacity statewide for students, parents, caregivers, teachers, and school partners to practice digital safety.

With the transition to virtual learning during the COVID-19 pandemic and the increase of technology mediated learning both at home and at school, comprehensive statewide student data protection is critical to ensuring safe, equitable learning environments. The chief student data steward will oversee the TED/LEA data lead and TED/LEA information security steward, while collaborating across departments to ensure strategic alignment.

#### **Responsibilities**

The chief student data steward's primary functions include, but are not limited to:

- ▶ Manage overall development and coordinate implementation of the New Mexico Public Education Department's privacy and data protection strategy and compliance plans in collaboration with key statewide stakeholders (e.g., chief information officer, procurement bureau chief, and advisory council)
- ▶ Continually evaluate school district standards and procedures. Train, educate, and communicate data protection standards and procedures; conduct risk assessments and develop and implement mitigation strategies; employ privacy auditing techniques to monitor and report on the program's effectiveness; and use data to identify trends and areas of risk
- ▶ Serve as a primary liaison for statewide TEDs/LEAs, vendors, and school marketplace partners
- ▶ Deliver trainings to educate and empower the New Mexico public education community regarding data protection concerns
- ▶ Review and edit student data protection agreements and vendor terms of use/service agreements

### Qualifications

Bachelor’s degree in public policy, computer science, management information systems (MIS), or information technology and two (2) years of experience in systems administration, or similar technical degree or certifications. Substitutions apply.

### Substitutions Table

	Education		Experience		Education		Experience
1	High school diploma or equivalent	<b>AND</b>	6 years of experience				
2	Associate degree in the field(s) specified in the minimum qualification	<b>AND</b>	4 years of experience	<b>OR</b>	Associate degree or higher in any field	<b>AND</b>	6 years of experience
3	Bachelor’s degree in the field(s) specified in the minimum qualification	<b>AND</b>	2 years of experience				
4	Master’s degree or higher in the field(s) specified in the minimum qualification	<b>AND</b>	0 years of experience				

### Ideal Candidate Skills

- ▶ Expertise in applicable education data regulations
- ▶ Familiarity with development and implementation of compliance best practices
- ▶ Experience in identifying, assessing, and mitigating privacy risks
- ▶ Experience in drafting reports for senior leaders to plan for, design, or enhance statewide systems for tracking compliance activities

### **TED/LEA DATA LEAD JOB DESCRIPTION**

The TED (Tribal Education Department)/LEA (Local Education Agency) data lead role will oversee student data protection protocols for school districts and charter schools.

With the transition to virtual learning during the pandemic and the increase of technology mediated learning both at home and at school, comprehensive statewide student data protection is critical to ensuring safe, equitable learning environments. The TED/LEA data lead will report to the state chief student data steward and work in close collaboration with the TED/LEA information security steward, while collaborating across school district and tribal departments.

#### **Responsibilities**

- ▶ Authorize and manage the sharing, deletion, and opt-out requests of personally identifiable student data for the school district
- ▶ Provide for necessary technical assistance, training, and support to all personnel and key stakeholder groups (students, parents, caregivers, and school partners) with access to student data
- ▶ Act as the primary local point of contact for the school districts and the chief student data steward
- ▶ Manage the notification process to ensure affirmative consent from parents, caregivers, and students about data sharing requests, procurement decisions, vendor agreements, revisions to terms of service, external research requests, etc.



### Qualifications

Bachelor’s degree in computer science, management information systems (MIS), or information technology, or similar technical degree or certifications and two (2) years of experience in systems administration. Substitutions apply.

### Substitutions Table

	Education		Experience		Education		Experience
1	High school diploma or equivalent	<b>AND</b>	6 years of experience				
2	Associate degree in the field(s) specified in the minimum qualification	<b>AND</b>	4 years of experience	<b>OR</b>	Associate degree or higher in any field	<b>AND</b>	6 years of experience
3	Bachelor’s degree in the field(s) specified in the minimum qualification	<b>AND</b>	2 years of experience				
4	Master’s degree or higher in the field(s) specified in the minimum qualification	<b>AND</b>	0 years of experience				

### Ideal Candidate Skills

- ▶ Expertise in applicable education data regulations
- ▶ Familiarity with development and implementation of compliance best practices
- ▶ Experience in identifying, assessing, and mitigating privacy risks
- ▶ Experience in drafting reports for senior leaders to plan for, design, or enhance statewide systems for tracking compliance activities

## **TED/LEA INFORMATION SECURITY STEWARD JOB DESCRIPTION**

The Tribal Education Department (TED)/Local Education Agency (LEA) information security steward will ensure that schools are developing and implementing a cybersecurity strategic plan and protocols to ensure student data protection.

With the transition to virtual learning during the pandemic and the increase of technology mediated learning and broadband access both at home and at school, comprehensive statewide student data protection is critical to ensuring safe, equitable learning environments. The TED/LEA information security steward will work in close collaboration with the TED/LEA data lead, while collaborating across school district and tribal departments.

### **Responsibilities**

- ▶ Oversee adoption of the Center for Internet Security controls and student data protection by design
- ▶ Provide information security training, technical assistance, and support to school personnel
- ▶ Conduct identity management to ensure that only authorized education personnel who have completed the appropriate training and education community data owners have access to the corresponding student data
- ▶ Establish data sovereignty tools and procedures to provide platforms for data owners to practice dynamic affirmative consent
- ▶ Establish data breach management protocols and oversee the Cyber Incident Response Team (CIRT)

## **ENDNOTES**

- 1 US Department of Education, "Frequently Asked Questions: Elementary and Secondary School Emergency Relief Programs; Governor's Emergency Education Relief Programs," May 2021, [https://oese.ed.gov/files/2021/05/ESSER.GEER\\_FAQs\\_5.26.21\\_745AM\\_FINALb0cd6833f6f46e03ba2d97d30aff953260028045f9ef3b18ea602db4b32b1d99.pdf](https://oese.ed.gov/files/2021/05/ESSER.GEER_FAQs_5.26.21_745AM_FINALb0cd6833f6f46e03ba2d97d30aff953260028045f9ef3b18ea602db4b32b1d99.pdf).
- 2 New Mexico Public Education Department, "Community Engagement," accessed December 5, 2021, <https://webnew.ped.state.nm.us/bureaus/teacher-family-outreach/>.
- 3 Barbara Pape, Jonathan Flynn, and Cecile Kidd, "Equity and ESSER: How Schools Can Embrace a Participatory Approach to Amplify Family Voices in Budget Planning," *Getting Smart*, June 30, 2021, <https://www.gettingsmart.com/2021/06/30/equity-and-esser-how-schools-can-embrace-a-participatory-approach-to-amplify-family-voices-in-budget-planning/>.
- 4 New Mexico Early Childhood Education & Care Department, "The New Mexico Early Childhood Strategic Plan 2021-2024," January 2021, [https://www.nmececd.org/wp-content/uploads/2021/01/2021-2024\\_NMEarlyChildhood\\_StrategicPlan.pdf](https://www.nmececd.org/wp-content/uploads/2021/01/2021-2024_NMEarlyChildhood_StrategicPlan.pdf).



**ASPEN TECH  
POLICY HUB**

**STUDENT DATA PROTECTION OFFICE**

Operational Plan