

Data Governance and IT: Tips for Communicating About Education Data Requirements

SLDS ISSUE BRIEF

June 2020

U.S. DEPARTMENT OF EDUCATION

A Publication of the National Center for Education Statistics at IES

This product of the Institute of Education Sciences (IES) Statewide Longitudinal Data Systems (SLDS) Grant Program was developed with the help of knowledgeable staff from state education agencies and partner organizations. The content of this publication was developed by the SLDS Data Governance and IT Collaboration Workgroup. The information presented does not necessarily represent the opinions of the IES SLDS Grant Program.

For more information on the IES SLDS Grant Program or for support with system development, please visit <http://nces.ed.gov/programs/SLDS>.

CONTRIBUTORS

Corey Chatis and Kathy Gosa, *SLDS Grant Program State Support Team*
Molly Abend and Tejal Cherry, *Maryland Longitudinal Data System Center*
Jamey Ereth, *Montana Office of Public Instruction*
Shane Hedani, *Hawai'i State Department of Education*
Tracy Korsmo, *North Dakota Information Technology Department*
Gayra Ostgaard, *Minnesota Department of Education*
Courtney Petrosky and Laura Wakefield, *Minnesota IT Services*
Margaret Leah Piatt, *Maine Department of Education*
Debbie Yedlin, *Arizona Department of Education*

Successful education data systems depend on developing a comprehensive set of requirements covering how the system will be constructed, managed, and used. These requirements should be informed by both the data governance groups that oversee the data system and the information technology (IT) professionals responsible for its development and operation.

This brief provides guidance for data governance and IT teams on communicating effectively about the requirements for education data systems and tools, including relevant content, standards, protections, and use. It offers tips for effective cross-team communication around six areas of data system requirements, along with examples from state data system teams.

Procuring Data Systems and Services

Data governance and IT teams need to establish clear roles and responsibilities regarding the process of procuring data system components and services from external sources. The procurement process includes creating requests for proposals (RFPs) and evaluating

potential vendors according to the customer agency's needs and policies.

Understand existing procurement requirements and processes

Data governance groups and IT teams both need a strong understanding of state and agency procurement requirements, processes, and related resources such as templates for documents like RFPs. Procurement often requires participation and expertise from both data governance and IT teams. Each group has different perspectives and areas of focus, but using the right tools and templates and knowing the correct steps and expected timeframes going into the process can help the two groups work together and avoid misunderstandings and missed opportunities.

Leverage the expertise of experienced team members

Take advantage of the knowledge and experience of data governance and IT team members who have been involved in procurement processes for previous projects. Consider identifying IT and data governance team

members who have been through the procurement process and asking them for advice, lessons learned, and potential pitfalls. Discuss the procurement process with them or ask them to review the draft RFP or other documents.

Determine acceptable platforms and leverage existing infrastructure

Establish a process for identifying and communicating acceptable technology platforms and using existing infrastructure in concert with the wants and needs of data governance groups, the IT team, and data system users.

Identify pre-vetted products and vendors

Ensure that the individuals involved in procurement are aware of vendors and products that have already been evaluated and verified as meeting federal and state privacy and security requirements.

Creating and Authorizing Contracts

Data governance and IT teams need to establish clear roles and responsibilities regarding the contracting process with vendors to ensure that all education data requirements are addressed.

Understand existing contracting rules and processes

Data governance groups and IT teams both need a strong understanding of state and agency contracting rules, processes, and related resources such as templates for contract documents.

State Example: Maine

Maine has a central, statewide Office of Information Technology (OIT) as well as a central procurement office outside of the Department of Education (DOE). Representatives from both OIT and DOE take part in data governance strategic planning discussions involving the procurement of new software and services or changes to existing systems. Under the state's procurement process, DOE's data team works with the state procurement office and the program that will own the system to write an RFP, select a bidder, and contract with the selected vendor. OIT provides technical consultation during the RFP process as well as technical support when contracts are reviewed.

Incorporate confidentiality documents into contracts

Confidentiality requirements of the federal Family Educational Rights and Privacy Act (FERPA) and other relevant regulations should be included as exhibits in all contracts. Both the data governance and IT teams need to provide input into relevant regulations and policies to ensure that nothing is missed and both perspectives are addressed.

Designate data governance and IT representatives to review contracts

Representatives from both data governance and IT teams should be involved in reviewing contracts to ensure that all applicable requirements are covered.

Ensure that agency processes are shared

When contracting with a vendor, make sure that expectations around processes such as data validation are clearly communicated among the agency's data governance and IT teams and the vendor company. A contract deliverable that documents the data validation rules and techniques to be used will help ensure that all parties understand the requirements and processes and can provide multiple layers of testing and certification.

Meeting Privacy Requirements

Data governance and IT teams both need to understand key concepts surrounding privacy requirements for data about students and children. These requirements are detailed in federal measures such as FERPA, the Protection of Pupil Rights Amendment (PPRA), the Health Insurance Portability and Accountability Act (HIPAA), the Individuals with Disabilities Education Act (IDEA), and the Children's Online Privacy Protection Act (COPPA). Additionally, state laws, agency policies, and the needs of local education agencies will dictate privacy protections that education data systems must meet.

Incorporate privacy and security requirements into product vetting

Develop a collaborative process between data governance and IT teams for ensuring that federal and state privacy and security requirements are considered when evaluating data system products and services.

Establish communications channels between data governance and IT

Ensure that there is an ongoing mechanism for the IT team to share information about state and agency security requirements with data governance groups. Likewise, there should be a mechanism for data governance groups to communicate to IT teams federal and state data privacy requirements such as nondisclosure obligations.

Refer to legal counsel

Engage the legal representatives who are knowledgeable about federal and state data privacy laws as needed to clarify requirements, or reference their legal resources and relevant legislation.

Aligning to Strategic Plans and Data Use Priorities

Data governance groups can help IT teams understand the agency's strategic plan and general priorities for data use, as well as how those priorities will affect the data system's technical infrastructure.

Develop strategic plans and data use priorities collaboratively

Data governance groups and IT teams both should be involved in creating the state or agency's strategic plan and setting data use priorities. Their involvement will

State Example: Hawai'i

The Hawai'i State Department of Education (HIDOE) emphasizes student privacy in all aspects of its work with data, including training for educators and staff, administrative processes, and IT guidance for software use. For example, agreements with vendors and third-party organizations that involve personally identifiable information from student records are reviewed by HIDOE's Data Governance and Analysis Branch as part of the procurement process. This review ensures that the agreements meet HIDOE requirements for privacy, security, and data management. When needed, the branch consults HIDOE's IT team to confirm that agreements also meet the department's technical needs. If vendors request language in contracts that differs from HIDOE's standard requirements, the Data Governance and Analysis Branch consults HIDOE's legal counsel before signing off on the changes.

State Example: Montana

The Montana Office of Public Instruction (OPI) draws on the stated priorities and initiatives of its leadership to develop strategic plans for its operations. OPI's *Data Use Priorities* document outlines four themes to guide education data use and research:

1. **General student outcomes** evaluates student performance and college and career readiness based on standards aligned to the state superintendent's strategic goals as well as shared policy objectives developed with the state Board of Public Education, higher education entities, and the state legislature.
2. **Special program effectiveness** examines the effectiveness of programs aimed at specific populations of students.
3. **University researcher projects** establish collaborative relationships between OPI and Montana University researchers.
4. **Teacher quality** encompasses partnerships with educator preparation programs to train future Montana educators to use data effectively.

OPI's *Agency Information Technology Plan* also directly references the superintendent's strategic goals and the state strategic plan to outline IT objectives to support those goals. Specifically, the IT plan lays out 6 goals and 18 supporting objectives related to developing capable and sustainable systems, supporting staff and building strong teams, improving communications and awareness, protecting and securing information, and controlling costs. Each goal and objective in the plan also references the element of the state and agency strategic plans that it supports.

During a recent reorganization, OPI established a single Data and Technology Division to combine the agency's data analytics and IT expertise and more effectively align the goals and objectives of both groups. Additionally, OPI's data governance program recently created a Data Use Committee composed of the agency's IT, data governance, and data analytics and research-driven program leaders. With guidance from the broader data governance program, the Data Use Committee will develop a structured approach to tracking and demonstrating progress toward meeting the goals of the *Agency Information Technology Plan*, *Data Use Priorities*, and OPI's federal SLDS grant.

help ensure that implications for IT infrastructure are identified proactively and that stakeholder needs and business requirements such as those related to federal and state reporting are integrated into the plans and priorities.

Communicate changes to plans and priorities

Data governance groups need to provide IT teams with a comprehensive overview of any changes to the state or agency's strategic plan or data use priorities so that infrastructure implications can be proactively identified.

Develop a road map for data

Data governance groups and IT teams should work together to create a road map or ongoing process to define and select the data components needed to support the agency's strategic plan.

Establish a holistic perspective on technical priorities

Data governance groups can help IT teams take a broad view of the agency's needs and technology environment in order to better align IT priorities and determine how they will add value to the agency's work. Similarly, IT teams can help data governance groups understand important technology requirements such as allocating resources for version updates, access controls, and product reviews in order to support the ongoing performance and security needs of the agency.

Develop standards to streamline technical decisions and processes

Data governance groups can work with IT teams to proactively set standards in areas such as data use and data visualization to inform decisions and processes about data system infrastructure.

Communicate plans for new and updated technology

IT teams should share with data governance groups ideas and plans for new infrastructure and system changes in order to gain input from data governance.

Understanding Agency and Data Governance Program Structure

Data governance groups can help IT teams understand the agency's overall organizational chart as well as the structure of the data governance program to clarify the individuals involved, the individual and group decisionmaking authority, and how data-related issues are escalated and resolved.

Data governance roles and responsibilities

Learn more about the roles and responsibilities of data governance groups in the SLDS guides *Single Agency Data Governance: Roles and Responsibilities* (<https://slds.ed.gov/#communities/pdc/documents/17092>) and *Interagency Data Governance: Roles and Responsibilities* (<https://slds.ed.gov/#communities/pdc/documents/17093>).

Document data governance roles, responsibilities, and authority

The roles and responsibilities of the various data governance groups and workgroups overseeing the data system should be formally documented, along with the authority of individuals within each group. This documentation will help IT teams and other parts of the agency know which staff members to contact.

Illustrate the roles and relationships among data governance groups

Data governance groups should provide IT teams with diagrams and visual representations to help

State Example: Minnesota

The data governance structure for Minnesota's interagency Statewide Longitudinal Education Data System (SLEDs) and Early Childhood Longitudinal Data System (ECLDS) consists of several working groups devoted to different aspects and uses of the data systems. Each working group has a chair or co-chairs responsible for filling out forms related to data requests, system updates, and questions about the data systems. These forms provide the basis for communications between the relevant working group and the broader data governance program as well as with IT representatives as issues move through data governance.

For most system updates and questions, the working group is recognized as the authority on a given project or initiative. The forms act as updates for other parts of the data governance program. IT representatives act on the direction of the responsible working group. IT representatives provide regular updates at the meetings of some data governance working groups. Other working groups consult with IT as needed.

explain the data governance groups, their respective decisionmaking authority and processes, and how they relate to one another.

Establish liaisons between data governance and IT

Data governance and IT teams should designate liaisons between their teams to ensure ongoing communications, including input into resolving issues.

Provide regular IT updates and ad hoc guidance

IT teams should provide regular data system updates at data governance meetings, and data governance groups should consult with IT teams as needed.

Adhering to Technical Standards and Policies

IT teams can help data governance groups understand the state and agency technical standards and policies that govern data systems, including around data security.

Make data privacy and security a regular part of collaborative meetings

IT teams can set a standing agenda item for meetings with data governance groups to share privacy and security information and updates.

Conduct ongoing reviews of access and authorization

IT teams should establish an ongoing mechanism to work with data governance groups to review and maintain IT authorization and user access to the data system. Regular access reviews help ensure that only authorized individuals can use specific components of—and data within—the data system.

Share state and agency security requirements

IT teams should ensure that there is an ongoing mechanism for communicating state and agency security requirements with data governance groups.

Conclusion

Requirements ensure that all aspects of education data systems, from procurement and construction to ongoing maintenance and data use, comply with legal obligations and support policy, practices, and agency needs. To develop and meet requirements, there must be ongoing, purposeful communications between data governance groups and IT teams in all areas. Above all, data governance and IT teams need to be proactive about collaboration and ensure that the right individuals are involved in planning, communicating, and implementing data system requirements.

State Example: Maryland

The Maryland Longitudinal Data System Center (MLDS Center) maintains a comprehensive *Data Security and Safeguarding Plan* for Maryland's P-20W+ (early childhood through workforce) data system. The plan details technical standards around data system access and authorization, privacy compliance, auditing, and data retention and disposal. It also covers policies and protocols around security awareness and training, security breach notification, risk assessment, systems configuration and management, and physical security for the MLDS Center's buildings and systems.

In addition to technical standards, the plan describes the MLDS Center's data governance groups and staff members, their roles and responsibilities, and the goals and guiding principles of data governance. A chart of the agency's data governance workflow is included in the plan.

MLDS Center leaders ensure that data governance and IT staff members are aware of key provisions in the plan that affect their daily work, such as transmitting data only through a secure file transfer system and updates to privacy compliance procedures. Privacy and security information is a standing agenda item for the agency's monthly Data Meetings. The *Data Security and Safeguarding Plan* is available publicly on the MLDS Center's website at <https://mldscenter.maryland.gov/egov/Publications/DataSecurity.pdf>.

Additional Resources

Hawai‘i State Department of Education

<http://www.hawaiipublicschools.org>

The Intersection of Data Governance and IT

Responsibilities: Self-Assessment Tool

<https://slds.ed.gov/#communities/pdc/documents/18451>

Maine Department of Education

<https://www.maine.gov/doe/home>

Maryland Longitudinal Data System Center

<https://mldscenter.maryland.gov/>

Minnesota Early Childhood Longitudinal Data System

<http://eclds.mn.gov/>

Minnesota Statewide Longitudinal Education Data System

<http://sleds.mn.gov/>

Montana Office of Public Instruction

<http://opi.mt.gov/>

SLDS Guide: Interagency Data Governance: Roles
and Responsibilities

<https://slds.ed.gov/#communities/pdc/documents/17093>

SLDS Guide: Requirements Traceability Matrix
Guide & Template

<https://slds.ed.gov/#communities/pdc/documents/19017>

SLDS Guide: Single Agency Data Governance: Roles
and Responsibilities

<https://slds.ed.gov/#communities/pdc/documents/17092>

SLDS Issue Brief: Effective Communications for
SLDS Teams

<https://slds.ed.gov/#communities/pdc/documents/5870>