Minnesota's Statewide Longitudinal Education Data System

(SLEDS)

Data Access

&

Management

Policy

April 7, 2014
DRAFT
Approved by
SLEDS Governance

Contents

Section 1 - Overview

Minnesota's Statewide Longitudinal Education Data System (SLEDS) brings together education and workforce data from the Departments of Education and Employment and Economic Development, and the Office of Higher Education to:

- Identify the most viable pathways for individuals in achieving successful outcomes in education and work,
- Inform decisions to support and improve education and workforce policy and practice, and
- Assist in creating a more seamless education and workforce system for all Minnesotans.

SLEDS will bridge existing education and workforce data. Using the 4P's — Pathways, Progress, Predictors and Performance, stakeholders will have a framework to assess and evaluate data from all systems in order to answer critical and long-ranging questions, while building a comprehensive body of information that can be used to inform future decision making.

1.1 Purpose

The purpose of this document is to support and promote greater understanding and use of SLEDS data. This policy provides a framework for SLEDS partners to properly manage data access in compliance with data security and other applicable policies, and state and federal law. The policy provides for transparency in data access and use.

Policy Statement

Access to SLEDS data will be as broad as possible, but will be governed by the following federal and state laws and resultant policies and procedures;

- Minnesota Government Data Practices Act (MGDPA, Minn. Stat.§ 13)
- Family Education Rights and Privacy Act (FERPA, 34 CFR Part 99)
- Confidentiality and Disclosure of Unemployment Compensation Data (CFR 20. Part 603)

See Section 1.4 for additional information about these statutes.

Additional factors that are considered when determining the level of access are:

- Classification of data,
- Role and responsibility of the user, and
- Compliance of users with data security policies and training.

1.2 Guiding Principles

Based on the work of the SLEDS Research and Data Advisory Committee, seven guiding principles for data access and management have been established:

1. **SLEDS will focus on providing cross-sector, linked data and analysis.**

    - This principle asserts that SLEDS focuses on cross-sector data use and refers any data requests limited to just one sector (K-12 education, postsecondary education or employment) to the appropriate agency or partner data provider.

2. **SLEDS relies on transparency and clarity in all we do.**

    - Education and workforce data, including its use, will be presented in plain and readily comprehensible language and formats. SLEDS partners will maintain a level of detail and disaggregation in accordance with state and federal regulations. SLEDS policies and procedures, including roles and responsibilities of all parties, will be defined and available for all to see.

3. **Protecting the privacy of individuals is a priority.**

    - This principle governs all we do and recognizes that an individual's privacy is a primary concern for contributing state agencies, partner data providers, and users of the SLEDS system. This requires users be aware of and respect the differing data privacy requirements of the various data sets included in SLEDS.

4. **Common understanding and use of data increases its value.**

    - This principle recognizes that only common understanding and use of data allows SLEDS to empower and inform decision making. This level of understanding requires contributing state agencies and partner data providers to jointly develop an understanding of and common language regarding the transitions between systems in addition to local programs. This process requires that state agencies and partner data providers discuss and commit to overcoming the obstacles to shared understanding and use of data, including but not limited to the issues of turf, trust, technology and time.

5. **Data providers, at the state and local levels, are critical sources for understanding and explaining the data.**
    - This principle recognizes that state agencies and partner data providers are critical sources for understanding and explaining data in SLEDS. Training and opportunities for data users to connect with data providers is imperative for success. Data users should be specific and transparent in describing their methodologies and assumptions and are encouraged to vet those methods and assumptions with contributing state agencies and partner data providers.
6. **Maintenance of SLEDS and the provision of research and analysis is the responsibility of all data providers.**
    - This principle recognizes that maintenance and use of SLEDS requires the coordinated and collaborative efforts of the contributing state agencies, the Minnesota P-20 Education Partnership and partner data providers.
7. **Local partner data provider access is needed for data to drive continuous improvement in local and state level policy.**
    - This principle recognizes that access to and use of data at the local level (i.e., colleges, K-12 schools and districts, workforce programs) is valued and better informs local improvement and state policy.

1.3 SLEDS Contact Information

Questions, requests for information, data access requests, and other SLEDS-related correspondence can be directed to any SLEDS Coordinators.

SLEDS website: xxxx
Minnesota P-20 Education Partnership: http://mnp20.org

Minnesota Office of Higher Education (OHE)
Meredith Fergus
Policy Analyst / SLEDS Coordinator
Meredith.Fergus@state.mn.us
651-259-3963
http://ohe.state.mn.us

Minnesota Department of Education (MDE)
Kara Arzamendia
Data Analytics Supervisor
Kara.Arzamendia@state.mn.us
651-582-8599
http://education.state.mn.us/

Minnesota Department of Employment and Economic Development (DEED)
Steve Hine
Research Director
Steve.Hine@state.mn.us
651-259-7396
http://mn.gov/deed/

1.4 General Information

SLEDS Data

As of October 1, 2013 SLEDS contains the following data.

K-12 Enrollment: Enrollment data aggregated at the school, district, county and state levels collected from Minnesota public and private K-12 institutions, including, but not limited to, enrollment by ethnicity, gender, grade and special populations. This data is managed by MDE.

K-12 Assessment: Results from statewide assessments such as Minnesota Comprehensive Assessment-Modified (MOD), Minnesota Test of Academic Skills (MTAS), Minnesota Comprehensive Assessment (MCA) and ACCESS for English Learners. Aggregated at the school, district, county and state levels, this data includes counts and percentages of students performing at four achievement levels. This data is managed by MDE.

ACT Assessments (Explore, Plan, and College Entrance assessments): ACT's Explore, Plan, and College Entrance assessment's results for Minnesota high school students in graduating classes from 2008 to 2012 aggregated at the district and high school level. These data were provided by ACT, and reflect only the most recent test results for students who tested on more than one occasion, and may include tests taken in grades 10, 11 or 12. This data is managed by MDE.

Adult Basic Education: Adult Basic Education serves students who are 16 years old or older, not enrolled in or not eligible to attend K-12 public or private school and lack basic skills in one or more of the following areas: reading, writing, speaking, listening and mathematics. Services provided include basic skills instruction, English for Speakers of Other Languages, General Educational Development (GED) preparation, adult diploma, work readiness, family literacy and transition to postsecondary education/training. This data is managed by MDE.

Advanced Placement (AP) Results: Advanced placement exam results are scores ranging from 1 to 5 and indicate the high school student's achievement level in the specified subject area. The scores are generally used by colleges to determine if the student will be granted college credit for completion of the AP course. This data is managed by MDE.

Kindergarten Readiness: Kindergarten Readiness Assessment data is information across developmental domains for a representative sample of public school

kindergartners across the state within the first several weeks of school. Data is collected by the child's teacher. This data is managed by MDE.

Early Childhood Enrollment: Early childhood enrollment includes children, birth to kindergarten, who: 1) either have an Individualized Education Plan (IEP),Individual Family Service Plan (IFSP), Individual Interagency Intervention Plan (IIIP) or received assessment for special education or 2) are pre-kindergarten students who are classified as grade- early childhood and have a primary disability. This data is managed by MDE.

GED Results: GED results include individuals who have passed the General Educational Development Test and received the State of Minnesota GED diploma. Individuals who take the GED are not currently enrolled in high school and do not have a high school diploma. In addition, test takers must be at least 19 years of age or at least 16 and have obtained an age waiver. GED results are based on a group of five subject tests which, when passed, certify that the taker has academic competencies similar to many of those required of a Minnesota high school graduate. This data is managed by MDE.

Postsecondary Enrollment: Fall term enrollment data collected from all Minnesota public and private postsecondary institutions, including but not limited to enrollment activity, program of enrollment, student level, student demographics, instructional activity, and secondary school information. This data is managed by OHE.

Postsecondary Completions: Degrees and other awards conferred data including information on degrees and other formal awards (diplomas or certificates) conferred to students upon successful completion of a program of study. This data is managed by OHE.

Institutional Characteristics: The Institutional Characteristics survey is administrated by the U.S. Department of Education and provides general information about postsecondary institutions. Data collected include: Institution address, telephone number, website, educational offerings, mission statements, control/affiliation, award levels, calendar system, and admissions requirements. Inclusion of the institutional characteristics data in SLEDS is managed by OHE.

U.S. Higher Education Enrollments and Completions (National Student Clearinghouse): Data on national higher education enrollments and completions is collected by the National Student Clearinghouse and provides information about the enrollment activity and degrees conferred by postsecondary institutions in the United

States. Inclusion of the National Student Clearinghouse data in SLEDS is managed by OHE.

Unemployment Insurance Wage Records: Data provided by all employers in Minnesota covered by Unemployment Insurance law. Data is provided quarterly and contains the names. Social Security numbers, wages, and hours of workers at each employer location. This data is managed by DEED.

Employer Detail: Data on all Minnesota businesses that describes their location, staff size, and primary industry. The North American Industrial Classification System (NAICS, http://www.census.gov/eos/www/naics/) is used. This data is managed by DEED.

Workforce Training Participant Data: Data on individuals who participate in workforce training programs. Data includes individual characteristics, and services provided. This data is managed by DEED.

Definitions

Contributing state agencies: Refers to the three state agencies with primary responsibility for SLEDS, including MDE, OHE, and DEED. Also included are the respective programs operated by the state agencies (e.g. Adult Basic Education operated by MDE).

Data: Categories of data in SLEDS ordered from most sensitive to least sensitive.

Individual-Level Data: Data on unique individuals.

Identifiable Linked Data: Original data from the contributing state agencies or partner data providers which are linked using personally identifiable information**.**

Personally Identifiable Information (PII): Data that identifies the individual. For the purposes of education records, PII is defined by federal law as information that includes, but is not limited to a 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 that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; and information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

De-Identified Data: Individual-level data that have enough personally identifiable information removed or obscured so that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify the individual. De-identified data will have are-identification code that allows the recipient to match information received from the same source.

Re-identification Code: A re-identification code enables an authorized researcher to return to the source of de-identified data and match the de-identified data to the source records. It is used when a researcher wants to link SLEDS data to additional data or refer to the original source data.

Anonymized Data: Anonymized data are individual-level data that have been de-identified and do not include a re-identification code and cannot be linked back to the original record system or other data.

Summary Data: Statistical records and reports aggregated from data on individuals in a way that individuals are not identified and from which neither their identities nor any other characteristic that could uniquely identify an individual is ascertainable.

Data Mart: Prepackaged data sets and reports.

Data Sharing Agreement: Statement signed by the contributing state agencies and one or more parties seeking to share data that outlines the purposes of the data sharing, legal restrictions, conditions and violations.

Data Usage Agreement: Statement outlining the appropriate uses of the data, which requires each user with access to SLEDS data to accept the conditions of use before being granted access to data or reports.

Directory Information: For the purposes of education records, federal law defines directory information as information contained in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed. Directory information includes, but is not limited to, the student's name; address; telephone listing; electronic mail address; photograph; date and place of birth; major field of study; grade level; enrollment status (e.g., undergraduate or graduate, full-time or part-time); dates of attendance; participation in officially recognized activities and sports; weight and height of members of athletic teams; degrees, honors and awards received; and the most recent educational agency or institution attended.

Education Records: Records that are: (1) directly related to a student; and (2) maintained by an educational agency or institution or by a party acting for the agency or institution.

MARSS number: Minnesota Automated Reporting Student System; Unique K-12 identification number assigned by MDE to each K-12 student.

Minnesota P-20 Education Partnership: The Minnesota P-20 Education Partnership is a voluntary organization made up of the statewide education groups in Minnesota, plus others from government, business, and other private sectors. Pursuant to its charter, the Partnership advises the contributing state agencies with regards to the governance of SLEDS.

MN.IT Services: The state agency responsible for setting information technology (IT) direction, standards and policies for the State of Minnesota, managing oversight and compliance of those standards, and providing IT services to all Minnesota state agencies.

Partner Data Providers: Organizations that provide data to a contributing state agency and agree to have this data used for or redisclosed to SLEDS. A list of the current Partner Data Providers can be found on the SLEDS website.

Research Partners: Individuals or organizations not categorized as contributing state agencies or partner data providers who have received authorization for research using SLEDS data.

SLEDS: Statewide Longitudinal Education Data System; refers to the data systems linking data from the pre-kindergarten to K-12 education to higher education to workforce creating a repository of data for informing education and workforce policy.

SLEDS Coordinator: Staff person at a contributing state agency responsible for coordination and management of SLEDS-related activity for the agency.

SLEDS Data Advisory Committee: The Data Advisory Committee members shall advise SLEDS with regard to technical expertise about data collection, data structure, data security and protocols for maximizing validity and reliability of SLEDS data. Membership of the SLEDS Data Advisory Committee is set by the Minnesota P-20 Education Partnership charter.

SLEDS Executive Committee: The Executive Committee is comprised of the commissioners or their designees of the three managing agencies having responsibility for SLEDS. This group is the final decision making body of SLEDS.

SLEDS Governance Committee: The Governance Committee members advise the contributing state agencies in regard to SLEDS-related research and evaluation to inform data-driven decisions and policy formation. This committee advises on additional data elements to be added to SLEDS, data security protocols, appointment of members to the Research Committee and Data Advisory Committees, approval of requests for accessing data, and assurance of access to public data in accordance with state and federal privacy laws. Membership of the SLEDS Governance Committee is set by the Minnesota P-20 Education Partnership charter.

SLEDS Research Committee: The Research Committee members advise SLEDS with regard to data system access, research and evaluation proposals, research

methodologies, and protocols for maximizing validity and reliability of SLEDS data. Membership of the SLEDS Research Committee is set by the Minnesota P-20 Education Partnership charter.

Source System ID: Refers to the ID used on individual person records by the data provider or state agency when submitting data to SLEDS. Where approved this ID allows new data to be linked to existing data or to refer to the original data source.

Sponsored Research: External requestors are designated as "sponsored research" if one or more contributing state agencies or partner data providers is supportive of its use of SLEDS data and provides a written statement of sponsorship as part of the requestor's Data Access Request.

Suppression Rules: Analytic techniques used for appropriately protecting private or confidential data. Methods involve removing data (e.g., from a cell or a row in a table) to prevent the identification of individuals in small groups or those with unique characteristics. This method may result in very little data being produced for small populations, and it usually requires additional suppression of non-sensitive data to ensure adequate protection of personally identifiable information. Suppression rules may apply to all summary reports or may apply to specific reports based on the combination of data elements included. Refers to standards set by the SLEDS Research and Data Advisory Committees[1] Best practices for data suppression for the purposes of appropriately protecting private or confidential data were issued by the U.S. Department of Education in 2011 (NCES 2011-603).

[1] TASK FOR COMMITTEE: Set STANDARDS

Maintaining the Privacy (Security) of Individual Information

There are many methods used to secure the privacy of individual-level data in SLEDS both at the system and user level.

MN.IT Services uses various procedures and security measures to ensure the confidentiality of an individual's records collected and maintained by SLEDS, including but not limited to:

- Assigning a unique SLEDS identification number to each individual,
- Managing Levels of Access that limit who may have access to data and for what purposes,
- Masking data to ensure that the confidentiality of personally identifiable information (PII) from individual records is maintained in all public reporting,
- Developing and maintaining a list of personnel who have access to personally identifiable student information through authentication and internal links,
- Implementing and maintaining appropriate administrative, technical, and physical safeguards that prevent any collection, use or disclosure of, or access to electronically maintained or transmitted individual records in SLEDS, and
- Ensuring all staff with access to SLEDS data understand the sensitivity and classification of the data and follow all requirements to protect the data from unwanted disclosure.

Contributing state agencies use various procedures and security measures to ensure the confidentiality of an individual's records collected and maintained by SLEDS, including but not limited to:

- Training of any personnel collecting and/or using personally identifiable information about the proper use of that information in accordance with this policy[2], Minnesota Government Data Practices Act (MGDPA), Family Educational Rights and Protection Act (FERPA), and all applicable state and federal laws and policies, [3]
- Enforcing a code of conduct for state employees, and
- Overseeing and managing all SLEDS-related work, policies and procedures to ensure compliance with data security standards, best practices, and federal and state laws.

[2] SLEDS-specific training to be developed by state agencies in conjunction with IPAD, will include documentation when training successfully completed.

[3] Include process for tracking completed training by SLEDS users within the Data Security Policy, MOU/data sharing agreements, and state agencies' SLEDS-related processes.

Levels of Access

SLEDS data must be consistently protected in a manner commensurate with its sensitivity and critical nature. The following levels of access describe the data available and have been developed to protect the privacy of individuals. A complete list of individuals with access to SLEDS by level will be maintained by MN.IT Services and the contributing state agencies. Access is approved by appropriate leadership. The access levels listed below are in the order of the most restrictive to the least restrictive:

Level 1A – allows specific MN.IT staff, including those housed at contributing state agencies, to read and write to all records and fields in the database. This access level is only permitted to a minimal number of authorized staff members who operate or manage the data system or are responsible for maintaining the accuracy and security of the data in the performance of their duties. Approval of access is granted by the appropriate contributing state agency commissioner or his/her designee and the OHE/MDE Chief Information Officer.

Level 1B – allows one agency staff person (non MN.IT) access to all records and fields within the identifiable liked data in order to manage the data system, manage reporting from the data system or maintain the accuracy and security of the data in the performance of their duties. The state agency's commissioner or designee approves access for the designated individual and signs the appropriate data sharing agreements before access is granted. Approval by the OHE/MDE Chief Information Officer is also required.

Level 2 – allows a minimal number of authorized DEED, MDE and OHE staff to access all records and fields of the identifiable linked SLEDS data. The requesting agency's commissioner or designee approves appropriate individuals and signs the appropriate data security agreements before access is granted. Suppression rules must be utilized by the researcher in production of summary level reports.

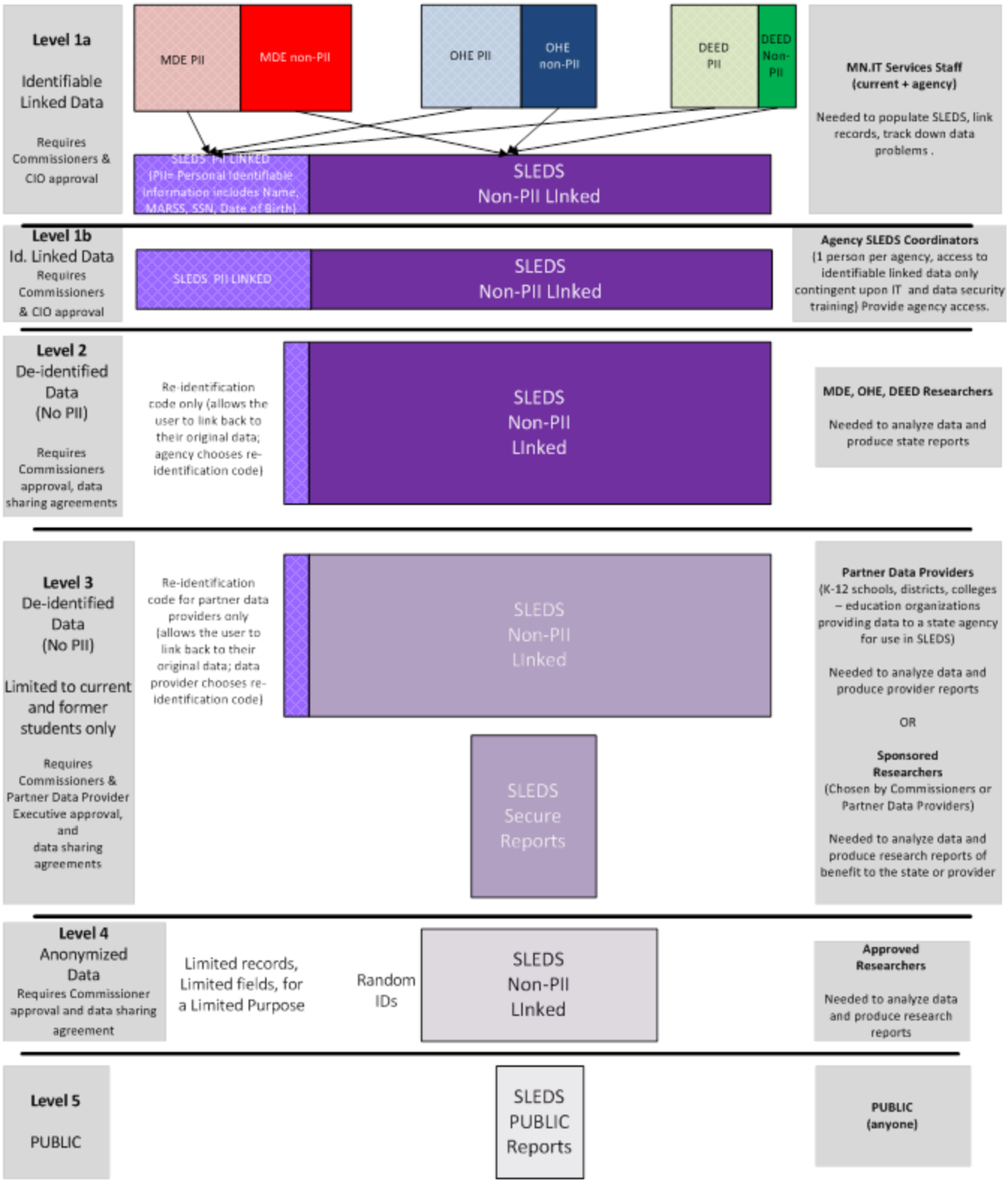
Level 3 – allows access to de-identified data, limited fields and secured reports. For approved research projects (partner data provider and sponsored researchers) access to data will be provided by data marts. Approval of access is granted by the contributing state agencies upon recommendation of the SLEDS Research Committee. Staff from partner data providers must also have approval from their organization's executive and sign the appropriate data security agreements before access is granted. Suppression rules must be utilized by the researcher in production of public reports.

Level 4 – allows for access to anonymized data in data marts to produce public reports. Suppression rules will be utilized with the use of data marts so that information

is not revealed about individuals in a particular group. Approval of access is granted by the contributing state agencies upon recommendation of the SLEDS Research Committee. Users must be approved by the contributing state agencies and sign a data sharing agreement or data usage agreement before access is granted. Suppression rules must also be utilized by the researcher in production of summary level reports.

Level 5 – allows access to the general public for viewing standard summary data. Requests for new public reports can be made to a SLEDS Coordinator.

Figure 1. Levels of Access Diagram



Record of Access

Data security standards and requirements of state and federal law mandate that agencies maintain a record of each request to and each disclosure of personally identifiable information from SLEDS. Such records must be maintained as long as the data are maintained, include the parties who have requested or received the information, and include the legitimate interests of the parties in receiving the information.

Unauthorized Access

A state agency that collects, creates, receives, maintains, or disseminates private or confidential data on individuals must disclose any breach of the security of the data following discovery or notification of the breach.

A “Breach of the Security of the Data” means unauthorized acquisition of data maintained by SLEDS. Good faith acquisition of government data by an employee, contractor, or agent of a state agency for the purposes of the state agency is not a Breach of the Security of the Data, if the government data are not provided to an unauthorized person.

“Unauthorized acquisition” means that a person has obtained data without the informed consent of the individuals who are subjects of the data or statutory authority and with the intent to use the data for nongovernmental purposes.

In the event of a “Breach of the Security of the Data” or possible “Breach of the Security of the Data” involving individual records or aggregate and distributional reporting of individual records disclosed for purposes of SLEDS, contributing state agencies will notify MN.IT Services as described in the standard (Enterprise Information Security Incident Management Standard 2010-01); notify the duly authorized representative of state agencies; notify the Governance Committee for the SLEDS; and notify any individual whose private or confidential information was, or is reasonably believed to have been, acquired by an unauthorized individual as required by Minn. Stat.§13.055.

Rights of Subjects of Data to Inspect and Review Data and Records

In compliance with state law, an individual who is the subject of stored private or public data on individuals may request to be shown the data without any charge and, if desired, be informed of the content and meaning of that data. In compliance with federal law, parents and eligible students have the rights to inspect and review education records. All records within SLEDS are managed by MDE, OHE and DEED and as such

those agencies are jointly responsible developing a policy for responding to all requests for access to SLEDS data and records in accordance with federal and state law.

Legislation Governing Data Sharing and Data Privacy

The majority of data in SLEDS is classified as private data by Minnesota statute. Private data can be used as necessary by the agencies that collect the data or have statutory authority to use the data. Private data cannot be disclosed except in specific situations. Federal regulations provide additional limitations to the use of certain data. Individuals found in violation of federal or state law or resultant policies and procedures are subject to consequences as documented in the Minnesota Government Data Practices Act (MGDPA), Family Educational Rights and Privacy Act (FERPA), and all data sharing and usage agreements for SLEDS.

Minnesota Government Data Practices Act (MGDPA)

The Minnesota Government Data Practices Act (MGDPA), Minnesota Statutes Chapter 13, asserts that all government data are public data unless classified otherwise. Public data can be disclosed to anyone for any reason. Private data, as designated under Minnesota law, may be collected, stored, used, or disseminated by government entities if the government entity is authorized to do so by state, local, or federal law (Minn. Stat.§ 13.05 sub.4(b); the individual subject or subjects of the data have given their informed consent; the data are being discussed at a meeting open to the public (see Minn. Stat.§13D.05). The majority of data in SLEDS are classified as private data, meaning their disclosure is limited to that authorized in statute. The use and preparation of summary data is permitted under Minn. Stat.§ 13.05 sub.7.

Education Data

In general, education data are classified as private under state law in Minnesota Statutes, 13.32, subdivision 1. "Educational data" means data on individuals maintained by a public educational agency or institution or by a person acting for the agency or institution which relates to a student. Pursuant to Minn. Stat.§ 13.32, subd. 11 the Minnesota Department of Education and the Minnesota Office of Higher Education have the authority to share educational data in order to analyze instruction in school districts for the purposes of improvement.

Adult Basic Education

Minn. Stat.§ 13.32, subd. 3(m) allows for the sharing of Social Security numbers of students in the Adult Basic Education program with the Minnesota State Colleges and

Universities and the Department of Employment and Economic Development for specified purposes.

Workforce and Training Data

Minn. Stat.§ 13.47 allows for employment and training data to be shared among providers to determine eligibility, and coordinate and improve services.

Unemployment Insurance

Data collected for administering unemployment insurance benefits, including wage data is private date with limited exceptions for disclosure under Minn. Stat.§ 268.19.

Family Educational Rights and Privacy Act (FERPA)

In compliance with the Family Educational Rights and Privacy Act, data for use in P-20W data systems such as SLEDS, requires that state agencies and partner data providers specify the conditions of use of data prior to inclusion. The conditions of use must include an anticipated data destruction date.

FERPA generally requires written consent of a parent or eligible student before an educational agency or institution discloses personally identifiable information. However, there are certain limited conditions in which prior consent is not required to disclose information (34 CFR Part 99.31).

These conditions include, but are not limited to, certain disclosures:

- To other school officials within the agency or institution determined to have legitimate educational interests,
- To officials of another school, school system, or postsecondary institution where the student seeks or intends to enroll or is enrolled for purposes of the student's enrollment or transfer,
- To authorized representatives of: 1) the Comptroller General of the United States; 2) the Attorney General of the United States; 3) the Secretary of the U.S. Department of Education; or 4) state and local educational authorities,
- In connection with financial aid for which the student has applied or received,
- To organizations conducting certain types of studies for, or on behalf of, educational agencies or institutions,
- If the information disclosed is designated as "directory information", or
- If the information disclosed has been stripped of all personally identifiable information and determined that a student's identity is not personally

identifiable after taking into account other reasonably available information (De-identified records and information).

For more information on the conditions under which prior consent is not required to disclose information, please see Title 34, §99.31, of the Code of Federal Regulations for FERPA. Organizations and individuals found to be in violation of FERPA shall be prohibited from accessing information from SLEDS for a period of five (5) years.

Destruction of Data

Any entity receiving personally identifiable information must destroy such data when it is no longer needed within the specified study time period or for the purpose for which the study was conducted. The manner of destruction shall protect the confidentiality of the information, and include the purging of all copies from computer systems. The SLEDS Research Committee must receive written confirmation of the method and date of destruction of data disclosed from SLEDS.

Section 2 - Procedure for Requesting Access to SLEDS

Access to SLEDS data requires all requesters, including researchers associated with contributing state agencies or partner data providers, must submit a completed *Data Access Request*.

2.1 Types of Requests

Contributing State Agency request

Contributing state agency researchers may request access to de-identified data (level 2 access, level 3 access) or anonymized data (level 4 access) for the purposes of research and analysis using SLEDS data as outlined by the Data Access Request Process beginning in section 2.2 of this document. Access to SLEDS data requires the requester agree to provisions set forth in the *Data Sharing Agreement* and complete the required data privacy and data security training prior to data access being granted.

Partner Data Provider request

Partner data provider researchers may request access to de-identified data (level 3 access) or anonymized data (level 4 access) for the purposes of research and analysis using SLEDS data as outlined by the Data Access Request Process beginning in section 2.2 of this document. Access to SLEDS data requires the requester agree to provisions set forth in the *Data Sharing Agreement* and complete the required data privacy and data security training prior to data access being granted.

External request – Sponsored research

External requestors are individuals or organizations who have research and /or academic credentials or associations. They are not associated with a contributing state agency or partner data provider. External requestors are designated as "sponsored research" if one or more contributing state agencies or partner data providers is supportive of its use and provides a written statement of sponsorship as part of the requestor's Data Access Request. External sponsored researchers may request access to linked, de-identified (level 3 access) or anonymized data (level 4 access) for the purposes of research and analysis using SLEDS data as outlined by the Data Access Request Process beginning in section 2.2 of this document.

Role of Sponsors

The role of sponsor is to:

- Provide a written statement that the requested research will contribute to the work of a contributing state agency or partner data provider and cannot be done using public research products,
- Participate in the Data Access Request development process,
- Provide subject matter expertise and assist with analysis, as appropriate, during the course of research, and
- Assist in assuring that the results of research are shared with appropriate stakeholders.

Sponsor information should be included in the Data Access Request.

Access to SLEDS data requires the requester agree to provisions set forth in the *Data Usage Agreement* or formal *Data Sharing Agreement* and complete the required data privacy and data security training prior to data access. An example of an external request for sponsored research would be TRiO programs requesting postsecondary outcomes of program participants as required for federal funding -- research supported by the Minnesota Office of Higher Education.

External request

External requestors are individuals or organizations who have research and /or academic credentials or associations. They are not associated with a contributing state agency or partner data provider. External requestors may be granted access to anonymized data (level 4 access) or summary reports (level 5 access). Summary reports will be made available on the SLEDS website. Requests to create new summary reports can be made to a SLEDS Coordinator in writing and do not require a Data Access Request. Requests for new summary reports may be subject to fees as determined by the contributing state agencies.

Public request

Summary reports (level 5 access) will be made available on the SLEDS website. Requests to create new summary reports can be made to a SLEDS Coordinator in writing and do not require a Data Access Request. Requests for new summary reports may be subject to fees as determined by the contributing state agencies. An example of a public / external, non-sponsored request would be a media request for data on postsecondary participation rates of high school graduates by school district.

2.2 SLEDS Data Access Request Information

This section reflects policies, practices and templates adopted by contributing state agencies, the Minnesota P-20 Education Partnership, and the SLEDS partner data providers to effectively respond to requests for data access. These procedures reflect sound principles set forth by the U.S. Department of Education, U.S. Department of Labor, other states, and the education, workforce and research community, for managing the flow of data, establishing research priorities, monitoring appropriate use, protecting privacy and ensuring that research efforts are beneficial to the state of Minnesota, contributing state agencies and partner data providers. All applicants requesting non-public data must submit a Data Access Request to be approved for access to SLEDS.

Roles and responsibilities

SLEDS Coordinators are charged with coordination and management of the Data Access Request Process. All requests for data access are received by a SLEDS Coordinator and forwarded to the SLEDS Research Committee for review and approval. All communication with the requestor is the responsibility of the SLEDS Coordinators**.**

The SLEDS Research Committee functions as a decision-making body and recommends approval or denial of a data access request. The SLEDS Research Committee recommends approval of access to SLEDS based on criteria authorized by the SLEDS Governance Committee. The SLEDS Research Committee is not an Institutional Review Board. The role of the SLEDS Research Committee is to screen data access requests to ensure they meet the criteria recommended by the SLEDS Governance Committee.

The SLEDS Governance Committee advises the SLEDS Executive Committee on standards for approving or denying access to SLEDS data.

The SLEDS Executive Committee has legal responsibility for approving access to SLEDS data and for the managing and securing the SLEDS data system.

Guidelines for Conducting SLEDS Research

Guidelines for the SLEDS Research Committee when reviewing requests for using SLEDS data are the following:

1. The study must involve analysis of transitions between systems or between providers within a system.
2. The study must be in alignment with state priorities.
3. The study must have the potential to make a definite contribution to contributing state agencies and partner data providers (e.g. study on impact of advising and college prep services to students at low-income public schools on high school graduation and college participation).
4. The researchers must use sound research design and have the potential for successful completion.
5. The project must comply with ethical standards for research in education and with all regulations set forth in federal and state law, particularly as they pertain to privacy of data on individuals.

Sensitive Data Elements

Some SLEDS data elements may be classified as “sensitive” based on “potential harm when used in contexts other than their intended use” per National Information Standards and Technology Special Publication 800-122 (2010). These classifications are noted in the data dictionary. Access to sensitive data elements may be limited in order to prevent potential harm or the identification of individuals as required by state and federal regulations. Access to sensitive data elements requires that the researcher submit a justification for inclusion of each requested data element as part of the Data Access Request.

Sensitive Data Elements include but are not limited to:

- K-12Enrollment: Disability category, disability type, homeless, migrant
- Postsecondary Enrollment: Institution name, Disability category, Citizenship status

Qualifying FERPA Exception

Requests for personally identifiable information must demonstrate that such information is required for purpose(s) of the study. In addition, requests must identify the qualifying FERPA exception allowing for personally identifiable information to be disclosed.

- **Studies Exception** allows for the disclosure without consent of personally identifiable information (PII) from education records to organizations conducting studies "for, or on behalf of," schools, school districts, or postsecondary institutions. These studies can only be for the purpose of developing, validating, or administering predictive tests; administering student aid programs; or improving instruction.
- **Audit or Evaluation Exception** allows for the disclosure of personally identifiable information (PII) without consent to authorized representatives of the FERPA permitted entities including Comptroller General of U.S., U.S. Attorney General, U.S. Secretary of Education, and state or local educational authorities. PII must be used to audit or evaluate a federal or state supported education program, or to enforce or comply with federal legal requirements of said education programs (audit, evaluation, or enforcement or compliance activity).

Human Subject Review

The SLEDS Research Committee shall ensure that data privacy and security standards established comply with standards for the use of human subjects. However, the SLEDS Research Committee is not an Institutional Review Board.

Cost Sharing

In anticipation of the number of data access requests received by SLEDS, the SLEDS Executive Committee has determined that the costs of preparing data related to data access will be passed onto the researchers or other entities requesting data.

Cost estimates are based on the standard salary of the IT programming staff members who perform this type of work, currently $70 per hour. SLEDS does not share costs related to data access if the request involves eight hours or less of SLEDS staff time.

The SLEDS Executive Committee may choose to waive all or a portion of the costs associated with preparing data for a data access request if the researcher or other entity is unable to pay the costs, or if the SLEDS Executive Committee determines that the data access request will result in a significant mutual benefit to the contributing state

agencies that warrants waiving IT-related costs. Each data access request is reviewed independently by the SLEDS Research Committee.

This policy is consistent with the Minnesota Government Data Practices Act, which authorizes government entities to charge requesters for certain costs related to accessing government data.

Timeline for Data Access Request Review

Data Access Requests are reviewed on a monthly basis. The initial review of access requests will take 6-8 weeks and the entire approval process is likely to take 4-6 months, depending on the quality, type of request, and number of data elements requested.

2.3 SLEDS Data Access Request Requirements

For Data Access Requests to be considered, researchers must submit a complete application.

Step 1: Submit a Complete Data Access Request

Each organization or individual requesting access to SLEDS must submit a completed *Data Access Request.* Requests may be submitted via the SLEDS web interface. Submission of the Data Access Request requires the requester acknowledge data privacy statutes set forth by FERPA, MGDPA, SLEDS conditions of use, and the penalties for violating the stated obligations. The requested data may only be used for the purpose of the research or study proposed within the timeframe requested. To request the same or different data for another purpose, a new *Data Access Request* must be submitted. SLEDS data is not to be used for survey purposes.

A *Data Access Request* must include:

1. Researcher contact information,
2. Research project title
3. Research project abstract describing the study and including:
    a. Purpose of research, including a description of its value to state policy, contributing state agencies, and partner data providers
4. Qualifying FERPA exception, if requesting personally identifiable data
    a. school official with legitimate educational interest,
    b. studies for, or on behalf of educational agencies or institutions to: (A) Develop, validate, or administer predictive tests; (B) Administer student aid programs; or (C) Improve instruction (34 CFR 99.31(a)(6)),
5. Theoretical background including references,
6. Description of the study which must include the following:
    a. Hypotheses or specific research questions to be addressed,
    b. the cohort or population to be studied,
    c. the data elements requested, including specific justification for inclusion of sensitive data elements, and
    d. a description of the methodology and analysis you propose to perform,
7. Any statement of sponsorship,
8. A list of all funding sources and budget for the study,
9. A time frame for completion, and
10. A signed statement of compliance with the SLEDS data security policy.

Data Access requests should be uploaded via the SLEDS Researcher website. Requests will be prescreened by a SLEDS Coordinator to ensure it includes all required

information. If any information is missing, the requester will be notified that the request is on hold until required information is submitted.

Step 2: Review by coordinators

In order to ensure clarity in requests, SLEDS coordinators will work with MN.IT Services to estimate fees and time required for fulfilling a Data Access Request. Upon review of this information with the requestor, SLEDS Coordinators will confirm the requestor's interest and forward the request to the SLEDS Research Committee

Step 3: Review by the SLEDS Research Committee

The SLEDS Research Committee shall review completed *Data Access Requests*.

Request Review Process

Once a completed *Data Access Request* is received, the SLEDS Research Committee will score the request by rating the following 8 elements on a scale of 0-5:

1. Analysis of transitions between systems or between providers within a system,
2. Addresses state priorities as defined by the SLEDS Governance Committee,
3. Have the potential to make a definite contribution to education and workforce research,
4. Quality and technical adequacy of the study design,
5. Appropriateness of the data analyses,
6. Evidence of research and writing competence,
7. Have the potential for successful completion, and
8. Probability of compliance with ethical standards for research in education and with all regulations set forth in federal and state law, particularly privacy of data on individuals.

The SLEDS Research Committee will review the proposal and make the recommendation for:

- Approval (30-40 points), or
- Revision (0-29 points).

Upon completion to the review process, designee scoring and comments shall be forwarded to the SLEDS Executive Committee.

Step 4: Final Approval Process

After reviewing the request and the recommendation from the SLEDS Research Committee, the SLEDS Executive Committee may respond to the request in one of three ways:

1. **Approve the request**: Upon approval of the Data Access Request[4], the requester will be contacted by a SLEDS Coordinator of the approval.
2. **Invite revisions to the request:** In some instances, the SLEDS Executive Committee may request additional information or ask that the requester to revise the *Data Access Request* in response to comments, questions, or suggestions from Research Committee members or to ensure compliance with data privacy statutes and the SLEDS data security policy. A SLEDS Coordinator will contact the requester with the Committee's revision request.
3. **Deny the request:** While it is the policy of the SLEDS Executive Committee to facilitate access to SLEDS data, the SLEDS Executive Committee may deny *a Data Access Request* which fails to meet the criteria established, violates data privacy law or SLEDS contractual obligations, if the requester refuses to comply with terms of use, data sharing agreements, or SLEDS data security policy, or if the requestor has violated data privacy law or refused to comply with applicable policies and procedures in the past.

[4] COMMMITTEE must decide on approval process (e.g. majority vote, unanimous) and be granted that authority by the Governance Committee

Acceptance of the terms of use

Once approved, permission to access the SLEDS data requires the requester to complete an online *Data Usage Agreement* or formal *Data Sharing Agreement* prior to data access.

Data Transfer

The approved data will be made available by MN.IT Services to the requester by secure means.

Step 5: Completion of Research

Completion of research requires the requester to submit research findings and comply with data destruction requirements, if applicable.

Submission of Research Findings

The *Data Usage Agreement* and *Data Sharing Agreement* requires that all requesters provide a SLEDS Coordinator with a paper and electronic report of final results no more than 30 days prior to publication of the study. The report will be forwarded by a SLEDS Coordinator to the SLEDS Research Committee, research sponsors, and the contributing state agency commissioners. After publication, the SLEDS Coordinator will forward the report to, the SLEDS Governance Committee and the SLEDS Document Library. Failure to submit a final report jeopardizes approval of future proposals. Publications emanating from studies using SLEDS data should acknowledge the contributions of SLEDS.

Data Destruction

Upon completion of the study time frame, each requester will be notified by the designated SLEDS coordinator that the study period has ended and that the data must be destroyed. The researcher must sign a compliance statement or send a letter to the agency coordinators that the data has been destroyed. If additional external data was submitted by the researcher for purposes of linking to SLEDS data, the SLEDS coordinator will issue a letter to the researcher that the data has been destroyed.

Report of Completed Research

It is the responsibility of the SLEDS Research Committee and the SLEDS Coordinators to provide the SLEDS Governance Committee, the SLEDS Executive Committee and

the Minnesota P-20 Education Partnership with a report on completed research. The SLEDS Governance Committee shall determine the schedule for reporting.

Section 3 - Policy Authorization

This policy was adopted by the SLEDS Governance Committee, the Minnesota Department of Education, Minnesota Department of Employment and Economic Development, and Minnesota Office of Higher Education.

This policy is effective <<month>> <<day>>, 2014.

Appendix A: Documents and Forms

A1. Data Sharing Agreement – Contributing State Agencies

A2. Data Access Request

A3. Data Sharing Agreement – Partner Data Providers and External Researchers

A4. Data Usage Agreement – External Researchers

A5. Request for New Summary Data to be Created

A6. Written Statement of Data Destruction Compliance

a. Researcher to SLEDS
b. SLEDS to Researcher