APPENDIX C: Documentation Pertaining to Data Security and Privacy

Facilitating Data Integration through Education Choice and Equity-Driven Research-Practice Partnerships

Wisconsin DPI Policies Related to Data Security and Privacy

- Open Records (1.130)
- Forms Management (4.200)
- Records Management (4.205)
- Student Data Access (4.300)
- Acceptable Use of Technology (4.105)
- Confidentiality of Individual Pupil Data and Redaction (4.315)
- Human Subjects Research (4.330)

DPI Information Technology Procedures

- IT Project Governance
- Internal Data Access Requests
- Local Security Access
- Data Contacts Inventory

DPI Researcher Access and Data Sharing

- Confidential Data Request Process and FAQ
- Data Use Agreement Template

State Laws and Regulations

- Pupil Records (Wis. Stat. § 118.125)

Other

- PTAC Review Feedback - from August 2019 SLDS Site Visit
- DPI Organizational Chart
- NIST Cybersecurity Framework

Wisconsin Department of Public Instruction
DEPARTMENTAL POLICY BULLETIN
PI-1100 (Rev. 07-09)

		Index **1.130**
Subject **OPEN RECORDS**	Effective Date **04/01/16**	Page **1 of 5**

A. Authority

Section 19.31, Wisconsin Statutes, provides for citizen access to information regarding the affairs of government and the official acts of government officers and employees. State agencies, as the custodians of official records, shall operate with the presumption of complete public access consistent with the conduct of governmental business.

Wis. Stats. §19.32(2)., defines a “record,” in part, as any material on which written, drawn, printed, spoken, visual, or electromagnetic information is recorded or presented, regardless of physical form or characteristics, which has been created or is being kept by an authority. Records created and maintained by this department are state property. A “record” does not include drafts, notes, preliminary computations and like materials prepared for the originator’s personal use or prepared by the originator in the name of a person for whom the originator is working; materials which are purely the personal property of the custodian and have no relation to his or her office; materials to which access is limited by copyright, patent or bequest; and published material in the possession of an authority other than a public library which are available for sale or which are available for inspection at a public library.

B. Records Custodians

The state superintendent, deputy state superintendent, executive assistant, and assistant state superintendents shall serve as custodians for records under their control and shall be ultimately responsible for responding to requests for review of records. Division directors or their designees shall handle requests for access to records under the supervision and direction of the respective records custodian and shall consult with the records custodian or legal counsel as needed in responding to records requests.

Records custodians shall be knowledgeable of the purpose for which records under their control are maintained, the general contents, and the location of such records. Reasonable restrictions may be determined and imposed by the records custodians on the manner of access to an original record if the record is easily damaged or irreplaceable.

A listing of records custodians, division directors, and types of records shall be available at the DPI Reception Desk, GEF 3.

C. Access to Employee Records

For purposes of the open records law, Wis. Stats. §19.32(1bg) defines “employee” as any individual who is employed by an authority (such as the Department of Public Instruction), other than an individual holding a state public office as defined in §19.42(13). Thus, for the purposes of the open records law, all employees of the department, including project employees and LTEs, are “employees,” except for the following positions (state public office holders):

- State Superintendent
- Deputy State Superintendent
- Executive Assistant
- Special Assistant (stenographer)
- Assistant State Superintendents (division administrators)

1. Unless otherwise authorized or required by statute, the following information about department "employees" will not be released in response to an open records request (unless the employee has consented to the release), pursuant to §19.36(10)(a) – (d).
   a. The employee's home address, home electronic mail address, home telephone number or social security number.

   b. Information related to a current investigation of a possible criminal offense or possible misconduct prior to the disposition of the investigation.

   c. Information pertaining to the employee's employment examination, except an examination score if access to that score is not otherwise prohibited.

   d. Information relating to one or more employees that is used for staff management planning, including performance evaluations, judgments or recommendations concerning future salary adjustments or other wage treatments, management bonus plans, promotions, job assignments, letters of reference or other comments or ratings relating to employees.

2. Unless otherwise authorized or required by statute, the home address, home electronic mail address, home telephone number or social security number of the department state public office holders, except for the State Superintendent, will not be released in response to an open records request (unless he or she has consented to the release), pursuant to §19.36(11).

3. If the department receives a request for "employee" records that are the result of an investigation into a disciplinary matter or possible employment related violation, and the investigation has been disposed of, the department will conduct the balancing test to determine whether the record must be released. If the department decides to release the information, it will notify the employee by personal service or certified mail, of the decision to release the information, a brief description of the records and a description of the rights of the employee to attempt to prevent the release of the information.

   If an employee receives such a notice, he or she shall have 5 days after receipt of the notice to provide written notification to the department of his or her intent to seek a court order restraining the release of the records. If the employee decides to seek court relief, he or she must file an action with the circuit court naming the department as the defendant, within 10 days of receiving the notice from the department. While the case is pending in either circuit or appellate court, the department will not release the records.

   If the department does not receive written notification of intent to seek court relief, the department will release the records 12 days after sending the notice to the employee.

4. Unless otherwise authorized or required by statute, if the department receives a request for records related to a state public office holder, it will conduct the balancing test to determine whether the record must be released. If the department determines to release the records, the department will provide the person written notice by personal service or certified mail of the decision to release the records, a brief description of the records and a description of his or her rights to augment the record. If a state public office holder wishes to augment the record after receiving such notice, he or she must

submit the written comments and documentation within 5 days of receiving the notice of intent to release the records.

D. Responding to Requests

Oral or written requests for access to records may be made at any time during normal business hours (Monday-Friday, 7:45-11:45 a.m. and 12:30-4:30 p.m.). A request shall be responded to as soon as practicable. Delaying access to a record or failing to provide a record may result in a penalty to the department. An area shall be provided for the requester to inspect records.

The department typically receives two kinds of records requests. The routine request that the staff person gets on a regular basis and broader requests that require assistance from other teams. Staff shall inform their supervisors of all records requests. When a request is non-routine, it should be forwarded or copied to the teams that it involves as soon as it is received. This includes notifying the department legal counsel. Because the law requires the department to respond to open records request as soon as practicable and without delay, it is imperative that the appropriate assistance is sought as soon as the request is received.

The department legal counsel will assist in responding to records requests or interpret the provisions of the open records law. The department forms and records coordinator can provide technical assistance, including determining the location of records stored off-site and directing the requester to the appropriate custodian. Requests from researchers and all requests for individual pupil data, including aggregate pupil data if the number of pupils in a given cell or group is five or less, shall be referred to the Chief Information Officer, Division for Libraries, Technology, and Community Learning (see Departmental Policy Bulletin 4.315). Requests for personnel information shall be referred to the Human Resources Director, Division for Finance and Management.

E. Fees

The records custodian shall collect fees that may be assessed for reproducing records. In general, the fee may not exceed the actual, necessary, and direct cost of reproduction or transcription of the record. The agency may not charge a fee for locating a record unless the actual cost is over $50. If a record contains information subject to disclosure and other information not subject to disclosure, the agency must separate one from the other, disclosing the one and withholding the other. The agency may charge the actual, necessary and direct cost of this redaction.

Fees for providing copies of records, not including sales tax, are as follows:

1. Fifteen (15) cents per page for photocopies.
2. The actual, necessary, and direct labor cost for transcription, photocopying, and shipping. This amount is calculated by multiplying the time spent to comply with the records request times the hourly rate and fringe benefits of the employee performing the work.
3. The actual, necessary and direct cost for postage, shipping or other delivery method.
4. The actual, necessary, and direct cost for locating a record if the cost is $50 or more.

5. The actual, necessary, and direct cost for computer programming and processing time. Sales tax shall be charged unless the requester is exempted by law from paying such tax.

F. Denial of a Request

Legal counsel must be consulted before a request for records is denied. When a request is denied in whole or in part, regardless of the method used by the custodian in arriving at that decision, the requester must be given specific reasons for denial. Following are general guidelines for denying requests:

1. Criteria for Denial
   a. The request does not reasonably describe the requested record or is without a reasonable limitation as to subject matter or length of time represented by the records, and the requester does not provide clarification.

   b. The record is specifically exempted from disclosure by state or federal law, s. 19.36.

   c. The custodian determines that the harm to the public interest in disclosing the record outweighs the presumed benefit to the public interest that would result from record disclosure. The "balancing test" may be used only when there is no law controlling records disclosure other than the open records law under Chapter 19, Wisconsin Statutes. If there is a need to restrict access at the time the request is made, the custodian may consider the exemptions to the open meetings law under §19.85.

   d. The request involves materials that are not records under §19.32(2), or by judicial decision or attorney general's opinion. A computer program is not subject to examination or copying, but the material or data used as input and the product are subject to the right of inspection and copying.

   e. The record involves advice from legal counsel concerning strategy, opinions, conclusions, or legal theories with respect to litigation in which the department is or is likely to become involved.

   f. The release of records would impede an open investigation.

Exceptions to the public record law should be narrowly construed. (*Hathaway v. Green Bay School District*, 116 Wis. 2d 388 (1984))

2. Procedures for Denial
   a. If an oral request is made, the custodian may deny the request orally unless a demand for a written statement of the reasons for denial is made by the requester within five business days of the oral denial.

   b. If a written request is denied, the custodian shall state in writing the reasons for denial. The denial must contain all the reasons for denial, because the agency may not be allowed to add reasons if the denial is challenged in court. The denial letter also must notify the requester of the following rights:
      1) Under §19.37(l), the requester may bring an action for a writ of mandamus asking a court to order release of the record. Under the same statute, the requester also may request, in writing, the district attorney of the county where the records are located or the attorney general to bring an action for a writ of mandamus asking a court to order release of the record.

2) The requester may wish to consult a private attorney concerning other remedies.

Questions regarding the open records law and this policy should be directed to the Office of Legal Services.

Wisconsin Department of Public Instruction
DEPARTMENTAL POLICY BULLETIN
PI-1100 (Rev. 10-03)

		Index **4.200**
Subject **FORMS MANAGEMENT**	Effective Date **03/08/06**	Page **1 of 2**

Section 16.61(2)(ad)(1) Wisconsin Statutes, defines “form” as every piece of paper, transparent plate, or film containing information which is printed, generated, or reproduced by whatever means, with blank spaces for the entry of additional information to be used in any transaction involving the state of Wisconsin.

A. Forms Review and Authorization

All forms developed by or under the sponsorship of the Department of Public Instruction shall be reviewed by the Data, Forms, and Records Management Section when initially proposed and annually thereafter; when a revision is proposed to add, delete, or change the content or format substantially; or when a related form is revised.

The authorization procedure consists of three phases:

- Data, Forms, and Records Management Section review and authorization
- State Superintendent Education Data Advisory Committee (SSEDAC) review (where required)
- Forms design

When a new or revised form is requested, the sponsor shall submit a draft to the department forms coordinator. The department forms coordinator should be consulted in the early phases of conceptualization and planning of new forms, major revisions of existing forms, and for technical assistance in data collection methods, data analysis, or preparation of data for automated processing in developing forms.

The department forms coordinator will determine whether a data collection request satisfies the authorization criteria and whether it must be referred to the State Superintendent’s Education Data Advisory Committee (SSEDAC). Data collection requests which are not based directly on law or regulation shall be referred to this committee.

Authorization is the determination that sufficient justification exists in law, regulation, or program need to permit the distribution of a data collection document/instrument. Data collections based directly on state or federal law or regulation shall be authorized by the department forms coordinator. Data collections not based directly on law or regulation shall be referred to the State Superintendent’s Education Data Advisory Committee (SSEDAC) for review.

The following criteria are considered in authorizing data collections:

1. Law or regulation implies the need for data collection in order to comply with a mandate, or data are necessary for managerial or legislative reporting or decision-making.

2. Data are not readily available from other sources within the department or from other state agencies.

3. The need for data as specified above outweighs the respondent burden to gather and report such data.

Forms should be scheduled for review and authorization as follows:

1. Annual Review and Authorization: Forms currently in use will be reviewed by the department forms coordinator each fiscal year. Forms will be authorized for a twelve-month period.

2. Changes in Data Collection Activities: Review and authorization shall be required when the following occur:

   - Revision of existing forms, subsequent to annual review and authorization, in order to add or delete or make changes to format.
   - Elimination or consolidation of one or more forms subsequent to annual review and authorization.
   - Development of new forms, including one-time surveys.

At least one week should be allowed for minor revisions and at least two weeks for comprehensive revisions of existing forms. At least six weeks should be allowed for the review and authorization of new forms, and at least one month for school district completion and submittal.

B. State Superintendent's Education Data Advisory Committee (SSEDAC)

The State Superintendent's Education Data Advisory Committee serves as the general coordinating body for public school and statewide data collection activities within the department. The committee consists of educational community representatives appointed by the state superintendent. By virtue of their positions, the department's chief information officer and the department forms coordinator also serve on this committee.

Forms requests referred to the committee shall be reviewed on the basis of the authorization criteria and forms coordinator recommendation. Requesting staff may be asked to appear before the committee to explain the need for the data. Following review, the SSEDAC chairperson will inform staff of the committee's recommendation.

C. Forms Design

Forms design entails the critical analysis of authorized requests and the use of accepted principles of forms design and survey research in developing a method and format for obtaining data which promote efficiency and simplicity.

Data, Forms, and Records Management Section staff will design the form and assign a form number after the review and authorization process has been completed. The form shall be subject to annual review and authorization.

Questions concerning this policy should be referred to the department forms coordinator.

Wisconsin Department of Public Instruction
DEPARTMENTAL POLICY BULLETIN
PI-1100 (Rev. 07-09)

		Index **4.205**
Subject **RECORDS MANAGEMENT**	Effective Date **04/01/16**	Page **1 of 1**

A. Definition

Wisconsin Statutes sec. 16.61(2)(b) defines “public records” as all books, papers, maps, photographs, films, recordings, optical disks, electronically formatted documents or other documentary materials, regardless of physical form or characteristics, made, or received by any state agency or its officers or employees in connection with the transaction of public business. “Public records” does not include:

1. Any state document received by a state document depository library.
2. Duplicate copies of materials—the original copies of which are in the custody of the same state agency and which are maintained only for convenience or reference and for no other substantive purpose.
3. Materials in the possession of a library or museum made or acquired solely for reference or exhibition purposes.
4. Notices or invitations received by a state agency that were not solicited by the agency and that are not related to any official action taken, proposed or considered by the agency.
5. Drafts, notes, preliminary computations and like materials prepared for the originator’s personal use or prepared by the originator in the name of a person for whom the originator is working.
6. Routing slips and envelopes.

B. Forms and Records Coordinator

The data, forms, and records coordinator in Information Technology shall assist department staff in establishing record retention periods and maintenance schedules and act as liaison to members of the public who seek information (Departmental Policy Bulletin 1.130, Open Records).

Department employees shall contact the data, forms, and records coordinator prior to destruction of any record unless otherwise authorized by a current records disposal authorization. The coordinator shall determine a suitable records retention period and process records disposal authorization through the Public Records Board. The Department complies with General Records Schedules approved by the Public Record Board to determine record retention periods and record disposal authorizations.

As designated in Wis. Stats. sec. 16.61 (2)(bm) the data, forms, and records coordinator shall serve as the liaison between the department, the Wisconsin Public Records Board, and the Wisconsin State Historical Society in all matters relating to record retention and destruction.

Questions concerning this bulletin may be directed to the data, forms, and records coordinator, Information Technology team, Division for Libraries, Technology and Community Learning.

Wisconsin Department of Public Instruction
DEPARTMENTAL POLICY BULLETIN
PI-1100 (Rev. 07-09)

Index
4.300

Subject	Effective Date	Page
STUDENT DATA ACCESS	**04/01/16**	**1 of 7**

A. Background

The purpose of this policy is to communicate the value of educational data and how student privacy and confidentiality is protected. An additional purpose is to document how student data is collected, maintained, and disseminated in compliance with applicable federal and state laws. The policy applies to all DPI divisions and teams, authorized agents and contractors, subcontractors and their agents.

The Wisconsin Department of Public Instruction (DPI) is required by law to collect and store student data to meet state and federal reporting mandates, e.g., the Every Student Succeeds Act (ESSA) (previously NCLB), Individuals with Disabilities Education Act (IDEA), and the Title II Higher Education Act. Data on student status and academic performance, linked to a unique and confidential Wisconsin Student Number (WSN) is collected annually from Wisconsin PreK-12 public school districts and 2r Charter Schools. Starting with the 2015-16 school year data are collected for choice students and private school students (if the school chooses to send private school data). Data are collected to fulfill federal and state required reporting as well as to empower students, educators, and families to make informed decisions to improve academic achievement and success in school. The DPI takes seriously its obligation to respect student's privacy and protect the confidentiality of the student data collected, used, shared, and stored by DPI. The DPI does not release or disclose personally identifiable student level data unless it is authorized by law.

To accompany this policy and provide guidance examples and best practices, refer to the Student Data Access Guidebook, which can be found on the DPI intranet site, on the "Data Access Request" pages or at the following link (https://fred.dpi.wi.gov/system/files/imce/workplace/it/_files/student_access_policy.pdf). This guidebook provides specific information needed to carry out the processes and procedures outlined in this policy.

B. Legal Consideration

The Federal Education Rights and Privacy Act (FERPA) applies to school districts that receive federal funds. The Wisconsin state pupil records law (s. 118.125, Wis. Stats.) applies to school districts; portions also apply to DPI. Additional restrictions on the disclosure of income eligibility status for subsidized lunches are provided in federal law under the jurisdiction of the US Department of Agriculture (USDA), and compliance is the responsibility of the local school district. The open records law also applies (see Departmental Policy Bulletin 1.130).

Student educational data should only be disclosed to those with legitimate educational reasons consistent with state and federal law. Furthermore, DPI believes that by implementing procedures for approving and granting access to student educational data adequately protects the confidentiality of individual pupils within the meaning of FERPA and the state pupil records law. Should a school district have any legal questions about disclosing pupil information, the district is advised to consult with its own legal counsel. More information on student privacy can be found within the DPI web site under the Student Data Privacy topic.

The following is a list of federal and state laws that govern the protection and privacy of education records and data:

Federal Laws

1. Children's Online Privacy Protection Act (COPPA)
2. The Family Education Rights and Privacy Act 20 USC 1232g, 34 CFR 99 (FERPA)

3. Individuals with Disabilities Education Act (IDEA) 34 CFR 300.560-300.577 (IDEA)
4. Richard B Russell National School Lunch Act 42 USC 1751Section 9 (B) (C) (D) (NSLA)
5. U.S. Department of Agriculture - Use of Free and Reduced Price Meal Eligibility Information Nondiscrimination or Identification of Recipients, 42 USC 1758(b)(2)(C)iii
6. Protection Of Pupil Rights Amendment (PPRA)
7. Uninterrupted Scholars Act Guidance

Wisconsin Law

1. Wisconsin Pupil Records Law (118.125)
2. Wisconsin's Data Breach Notification Law (section 134.98 of the Wisconsin Statutes)

C. Policy

Ownership of the Data

The PreK-12 public school districts and 2r charter schools are the originators and owners of the student educational data. The State Superintendent functions as the custodian of the data at the DPI. In order to protect the security and privacy of the data in its custody, DPI has established this policy to ensure that all data are securely maintained with safeguards on all personally identifiable or confidential information.

Process for Maintaining the Student Data Access Policy

The DPI's Data Privacy and Governance Committee (DPGC) partners with US Department of Education's Privacy Technical Assistance Center (PTAC) to monitor changes in state and federal regulations that relate to data collection, retention, privacy and reporting. As federal and state regulations change the DPI updates data security and privacy guidance and informs DPI staff and school districts through various modalities.

Measures Used by the DPI to Protect Student Data Privacy and Confidentiality

1. **Data Collection Process**
   a. The DPI has implemented rigorous authentication and authorization procedures to the data collection process.
   b. The data collection process at DPI is dependent on the same authorizations for access as those identified in the External Use and Access of data in section F below.

2. **Data Security**
   a. Security includes the technical measures put in place by the State of Wisconsin to ensure that records are not lost, stolen, vandalized, illegally accessed or otherwise rendered useless. Since the data are stored on servers and the network, procedures used include secure firewalls, transport layer security, audit trails and physical security, such as restricted server room access. All servers containing confidential educational data are managed by the DPI's Information Systems, Security, and Infrastructure (ISSI) team, and are secured to acceptable industry best practices and standards. All State of Wisconsin and federal security policies shall be followed and regularly audited. b. Breaches in Security
      1) Wisconsin's Data Breach Notification Law (section 134.98 of the Wisconsin Statutes) requires the DPI to notify individuals whenever personal information held by the DPI is acquired by an unauthorized person. However, no notice is required if the unauthorized acquisition does not create a material risk of identity theft or fraud, or if the information was acquired in good faith by an employee or agent and is used for a lawful purpose of the entity.
      2) The process for the DPI Data Incident Procedure can be found in the Data Access Guidebook.

3. **Data Redaction for Data Requests and Public Reporting**
Data Redaction is the process of masking the data displayed (i.e., putting an asterisk * in place of the actual number) to protect student privacy. For a complete description of DPI policy regarding data redaction refer to Department Policy Bulletin 4.315 Confidentiality of Individual Pupil Data and Data Redaction. Different software applications may utilize different redaction techniques depending on the tool being used, the data being displayed, and the way that the data is being combined for display. Each redaction technique has been vetted within DPI and through other groups like PTAC to ensure that each software application meets the applicable privacy laws to ensure that student privacy is protected. Additional guidance on redaction can be found in the Data Access Guidebook.

4. **A Unique Student ID**
The Wisconsin Student Number (WSN)/WISEid is a unique number assigned to each public school student, choice students, and some private school students. The Wisconsin Student Locator System (WSLS)/WISEid software application is used to assign a WSN/WISEid. The WSN/WISEid is intended to be a student's sole identifier throughout his/her PreK-12 experience. Due to federal and state reporting requirements, parents cannot opt their child out of being assigned a number in the system.

5. **Web Access Management System (WAMS) Wisconsin User ID**
The state's WAMS ID is a unique ID that allows individuals, once authorized by a security administrator for a specific software application, to access that application using the same means of identification for all applications to which they have been granted permission. When access to information or services is restricted, to protect an individuals' privacy or the privacy of others, users are asked to provide a Wisconsin User ID and password. Residents can register for the State's WAMS ID at the following web site: http://dpi.wi.gov/sites/default/files/imce/wisedash/pdf/wams-guide.pdf.

6. **External Access and Use of Data**
a. District/School Authentication and Authorization
    1) School district personnel may access through secure data collection and reporting tools individual student data and aggregate student data for those students currently enrolled in that specific district.
    2) DPI implements rigorous procedures for accessing data in all secure software applications and tools available through the Secure Home Portal, including WISEdash for Districts, from the district personnel perspective. (For additional information go to DPI's Secure Home Information Page.) Access to the data by school district personnel is controlled at the individual district level. Access is assigned based on a user's WAMS ID.
        a) Through DPI's Secure Home application, high ranking district personnel, either the District
        Administrator or their designee, are verified and granted District Security Administrator (DSA) access by specified DPI personnel after completing the District Administrator Authorization Form.
            i. The District Administrator Data Access Authorization is a binding agreement to which the District Administrator is acknowledging his/her responsibility and accountability for the misuse of this data by the users who have access within

his/her district whether the access has been assigned directly or via a designee. Additionally, the District Administrator agrees to authorize access to users of DPI's software applications within his/her district, or delegate the administration of this task, in accordance with the provisions contained within the District Administrator Data Access Authorization agreement.

ii. The DSA can assign Application Administrator access to specified district staff members. Application Administrators, in turn, can grant application access to individual educational personnel. More information is available on the District Personnel and Data Users page.

iii. DPI Application Security Manager (ASM) allows District Security Administrators and Application Administrators to securely assign or revoke user access to secure applications accessed through Secure Home. Examples of applications currently using Secure Home/ASM include the Postsecondary Transition Plan (PTP), Secure Access File Exchange (SAFE), School Directory, and WISEdash for Districts.

b) Each time a user attempts to log in to a secure software application, the WAMS ID is authenticated. Once authenticated, the staff member is allowed only to perform tasks within the data collection system based on the level of authorization designated in ASM or Delegated Authority. To further ensure security, the data collection systems require the staff member to log in again after a period of inactivity when using the software application.

i. As a condition of access, the local staff must agree to maintain the confidentiality of the data by signing an Application Usage and Data Access Agreement upon initial access to Secure Home. Users are regularly prompted to agree to this agreement throughout the duration of their access to the software applications and tools within Secure Home (for more information please see the following link: Security Overview)

7. Internal Access and Use of Data

a. Access Authorization

Staff employed by or under contract to DPI must receive authorization to access individual student data and/or aggregate student data that may be personally identifiable by their immediate supervisor. b.

Internal DPI Employee Data Access

1) The DPI Internal Data Access Request Process is developed for DPI personnel and contractors to request data access, to document approvals for access, and to monitor authorizations to DPI databases (e.g., LDS ODS, etc.) and software application tools (e.g., WISEdash, SAFE, etc.). Before access is granted, the requestor is required to complete Student Confidentiality Training, create a Data Access Request, and have the request approved through the hierarchy defined in this policy and documented in the DPI Internal Data Access Request Process. If the request is for data access through a software application, the requestor must also obtain a valid WAMS ID which is used to establish the security in ASM.

2) Types of Access
a) Continuing Access

Continuing access allows staff employed by or under contract to DPI to perform necessary tasks specified in their position descriptions or within the context of official DPI business, or relevant to accomplish a DPI task. This access is valid while the job duties remain the same. A change in job duties requires an updated access request form to be submitted to either revoke all access or for authorization to be updated and/or additional access provided. b) Limited Term Access

Limited term access allows staff employed by or under contract to DPI to perform a special or specific task for a pre-approved purpose for a specific limited duration.

3) Minimum Requirements Before Access is Authorized
Prior to accessing the student data, staff employed by or under contract to DPI must complete a training course in maintaining data confidentiality and sign an agreement, within the Internal Data Access Request form, to maintain the confidentiality of the data. Due to the sensitive nature of various data that DPI is mandated to collect additional authorizations and/or agreements may be required beyond those identified in this policy.

4) Use of Data
Authorized staff may use the student data only for the purposes for which access was granted.

8. Parent and Eligible Student Access

The Family Educational Rights and Privacy Act (FERPA) requires school district personnel to provide individual student data access to the parent of a minor child or to the eligible student as described in 34 CFR 99.10. Parents do not have access to DPI secure tools, but they have the right to access their student's records. Districts are encouraged to provide student records upon request within FERPA guidelines using the tools made accessible to them by DPI.

9. Non-Public Data Requests / Confidential Data Requests

a. Disclosure of Personally Identifiable Student Data

1) Access to all sets of individual student data and aggregate student data that may be personally identifiable is restricted. Access is granted only to individuals in the following groups, who have received authorization in accordance with this policy: a) Staff employed by or under contract with DPI,
   b) School district(s) where the student is currently enrolled,
   c) Parents, legal guardians and eligible students,
   d) Nondistrict personnel operating under appropriate institutional backing, within the limits of a binding DPI data use agreement, with legitimate educational interest as defined by FERPA. (34CFR § 99.3).

2) No individual student data or aggregate student data that may be personally identifiable shall be shared without the authorization of the Data Request Review Board (DRRB, see Section i[iii] below) and without a Data Use Agreement (DUA) in place.
   a) The DRRB considers and reviews all requests to conduct research using Wisconsin's student or school system data collected by DPI. Potential users such as doctoral and master's degree

candidates, university faculty, independent researchers, and private and public agencies must submit requests before receiving data and conducting and publishing their research.

b) Based on each request, the DRRB reviews the uses of the data to ensure that any products that are a result or outcome do not include personally identifiable data. For instance, data may be considered “de-identified” when all identifying characteristics have been removed from the data and all resulting sets of data are no longer linked or linkable to the individual student for whom the data was about or the data has been aggregated into a large enough pool of data that a student’s identity cannot be inferred.

c) Those requesting data must meet all of the DRRB’s criteria prior to obtaining access to any identifiable student-level data from DPI. One of these criteria is that the researchers have completed training on the ethical and professional standards for protecting human research participants that is either the same as or equivalent to the training that Department employees complete.

3) In compliance with the Family Rights and Privacy Act (FERPA), DPI does not disclose personally identifiable information from student records unless the disclosure is for one of the limited purposes outlined in FERPA, 20 U.S.C. § 1232g; 34 CFR Part 99:

a) Educational Studies: Student information may be disclosed to organizations conducting studies for, or on behalf of, DPI to: (1) develop, validate, or administer predictive tests; (2) administer student aid programs; or (3) improve instruction. Disclosures for the purposes of such studies must ensure that the study is conducted in a manner that does not permit personal identification of parents and students by individuals other than representatives of the organization that have legitimate interests in the information, the information is destroyed when no longer needed for the purposes for which the study was conducted, and DPI enters into a written agreement that meets the requirements outlined below.

b) Audits or Evaluation Activities: Student information may be disclosed to authorized representatives of DPI in connection with an audit or evaluation of federal- or state-supported education programs, or for the enforcement of or compliance with federal legal requirements that relate to those programs. Disclosures for the purposes of such audits, evaluations, or compliance activities must ensure that DPI uses reasonable methods to ensure that its authorized representative:

i. Uses personally identifiable information only to carry out an audit or evaluation of federal- or state-supported education programs, or for the enforcement of or compliance with federal legal requirements related to these programs;

ii. Protects the personally identifiable information from further disclosures or other uses, in accordance with FERPA;

iii. Destroys the personally identifiable information in accordance with FERPA; and

iv. iv. DPI enters into a written agreement that meets the requirements outlined below.

b. Data Sharing Agreements

1) The DPI Data Warehouse and Decision Support Team has a standard Data Sharing Agreement form that shall be used when DPI enters into agreements for research studies and audits or evaluations of federal- or state-funded programs.

2) FERPA regulations on the studies exception requires that the educational agency or institution or the State or local educational authority or agency headed by an official listed in 34 CFR §99.31(a)(3) execute a written agreement with the organization conducting the study when disclosing personally identifiable information from education records without consent. See 34 CFR §99.31(a)(6)(iii)(C).
3) FERPA regulations on the audit or evaluation exception require that the State or local educational authority or agency headed by an official listed in 34 CFR §99.31(a)(3) must use a written agreement to designate any authorized representative other than an employee allowed access to the data.

c. Data Request Review Board (DRRB)

1) To ensure the confidentiality of all student data while facilitating access to the data, DPI designates appropriate staff to serve on the DRRB.
2) The DRRB functions as a resource on federal and state law concerning student data confidentiality. The major responsibilities of the DRRB include: a) authorization of access to confidential student data;
   b) review and approval of the data collection processes for all confidential student data collections;
   c) review and approval of all data storage designs to ensure data confidentiality;
   d) review of the public reporting of student data to ensure student confidentiality within and across reports;
   e) monitoring compliance with all policies addressing student data confidentiality; and
   f) receipt and resolution of complaints regarding access, storage, and disclosure of student data.
3) Additional data security duties of the DRRB include but are not limited to the following:
   a) Training for staff and individuals under contract to DPI on student privacy and data confidentiality;
   b) Tracking staff access to student data and removal of limited term access when access periods expire or employee’s duties change;
   c) Assisting DPI management in developing contracts that may include student data access; and
   d) Assisting with approval/disapproval of external research requests.

Questions concerning this policy should be directed to the Chair of the DRRB.

10. DPI Staff Training

a. All new DPI employees and contracted staff must sign and adhere to the DPI Policy 4.105 Acceptable Use of Technology, which describes the permissible and unacceptable uses of state technology and information.

b. DPI requires all new employees to complete training during their first week of employment. The training contains information about DPI's structure and leadership, the responsibilities of a state employee, DPI policies and procedures, and where to find resources. A portion of the new employee training covers the topic of Personally Identifiable Information (PII).

c. DPI requires targeted security training for specific staff within DPI based on their roles.

d. DPI provides updated guidance and training to school districts regarding compliance with federal and state privacy laws and best practices. Information about such resources and guidance are posted to the DPI web site (see Student Data Privacy).

Wisconsin Department of Public Instruction
DEPARTMENTAL POLICY BULLETIN
PI-1100 (Rev. 10-03)

		Index **4.105**
Subject **ACCEPTABLE USE OF TECHNOLOGY** (Replaces 4.130 and 4.305)	Effective Date **7/27/07**	Page **1 of 6**

This policy supports the process of signing the Appropriate Use of Technology Sign-off Sheet (PI-1180-A) that every employee signs.

A. Overview

Department staff and other authorized users are required to utilize personal computers and other information technology resources in a manner consistent with the administrative, informational, instructional, and research objectives of the department and with respect for the public trust through which they have been provided. These resources may not be used in any manner, which violates the department policies, laws or statutes.

Access to the networks and to the information technology environment is a privilege and must be treated as such by all users of these systems. The integrity and stability of this resource is the shared responsibility of its users who must guard against abuses, which may disrupt and/or threaten the long-term viability of the systems. The department requires that all users act in accordance with these responsibilities, this policy, relevant laws, contractual obligations, and the highest standard of ethics.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, internet browsing, and FTP, are the property of DPI. These systems are to be used by authorized users for business purposes in the course of normal operations that serve the interests of the Department. Effective security is a team effort involving the participation and support of every DPI employee and affiliate who deals with department information and/or department information systems. It is the responsibility of every computer user to understand and implement the policy and guidelines.

B. Purpose

The purpose of this policy is to outline the acceptable use of DPI computer hardware and software by DPI employees and authorized non-DPI employees, including contractors and vendors. These rules are in place to protect the user and DPI. Inappropriate use of computer systems, including the improper use of passwords (see Passwords Departmental Policy Bulletin 4.100) exposes the DPI to risks, including compromise of network systems and services, and legal issues.

C. Scope

This policy applies to DPI employees and other authorized users, including vendors or contractors, who use any computer hardware and software that is owned or leased by DPI. All department staff having access to personal computers and other information technology resources are required to have a signed and dated *Appropriate Use of Technology Sign-Off Sheet (PI-1180-A)* on file with the Human Resources team. All other authorized computer users having access to personal computers and other information technology resources are required to have a signed and dated *Acceptable Use Policy Sign-Off For Non-DPI Employees (PI-1180-B)* on file with the Technology Services team.

D. Policy

General Use and Ownership

While DPI's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the department systems remains the property of DPI. Because of the need to protect DPI's network, management cannot guarantee the confidentiality of information stored on any network device belonging to DPI.

Users are responsible for exercising good judgment regarding the reasonableness of personal use. Users should be guided by departmental policies. If there is any uncertainty, users should consult their manager, Technical Services, or in the case of non-DPI employees, their DPI employee contact.

For security and network maintenance purposes, authorized individuals within DPI may monitor equipment, systems and network traffic at any time. DPI reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

1. Downloadable Software Applications

Downloadable software applications (including Internet browser plug-ins and tools) typically become locally resident on a desktop computer hard drive and may produce technical problems by conflicting with other software applications required for DPI business needs. Unapproved software may also introduce spyware software capable of capturing sensitive data. As is appropriate for any software loaded on any DPI computer, Technology Services staff should be involved in all software testing, documentation, training, and installs to ensure compatibility with DPI’s computing environment and manage technical support resources to meet DPI’s business needs. All staff requests for software applications should be reviewed by the appropriate team supervisor and routed to the Technology Services Team for assessment. Non-approved software may be removed at the discretion of Technology Services.

2. Hardware Security

Cables: A cable security system shall be installed for each laptop that anchors the laptop to an appropriate work surface to discourage casual or opportunity-type theft.

Data Storage: Diskettes, CD-ROMs, Zip Drives, Thumb Drives or other data storage devices that contain confidential information should be locked in a desk or drawer or located in a secured area such as a locked office.

Diskette or CD Replacement: Frequently used data disks or CD-ROMs should be replaced once a year. Old disks or CD-ROMs should be erased and discarded when no longer usable. Disk labels shall be marked with the date of initial use or formatting.

Equipment Modifications: Modification to the hardware configuration without the knowledge of the department system/network administrator is prohibited.

Inventory: A complete inventory shall be taken of all computer and computer-related equipment. The inventory shall be held and maintained by the Technology Services Team. This inventory shall be upgraded periodically to reflect current program area system configuration. All new equipment shall be tagged and added to the inventory.

Surge Protection: All computer and peripheral power cables shall be plugged into surge protectors.

4. Software and Data Security

Although Information Technology staff within the department provide and preserve security of files, security can be breached through actions or causes beyond their reasonable control. Department staff are required to safeguard program data, personal information, passwords, authorization codes, and confidential data, to take full advantage of the file security mechanisms built into the computing systems, and to follow the security procedures established to control access to and use of the systems.

Backup: Backup copies of software programs and data files stored on the network servers are made nightly by the local area network administrator. Copies of these backups are stored off site.

Contingency Plan: Technology Services staff stores at least one complete backup of all software and data files off site.

Data Access: Where sensitive data are involved, security measures shall be taken to monitor access to software and data.

Documentation: Applications shall be documented in such a way that another user could be easily trained and the applications recreated without difficulty.

Inventory: A complete inventory shall be taken of all software packages installed on department computers. This inventory shall be held and maintained by the Technology Services Team and shall be upgraded periodically.

5. Unacceptable Use

The following activities are prohibited. Under no circumstances is a user of DPI-owned resources authorized to engage in any activity that is illegal under local, state, federal or international law.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

<u>System and Network Activities</u>

The following activities are strictly prohibited, with no exceptions:

a. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by DPI.
b. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which DPI does not have an active license is strictly prohibited.
c. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).
d. Using a DPI computing asset to actively engage in procuring or transmitting material that is in violation of DPI's sexual harassment policy or any other sexual harassment or hostile workplace laws in the user's local jurisdiction.
e. Making fraudulent offers of products, items, or services originating from any DPI account.
f. Making statements about warranty express or implied.
g. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
h. Port scanning, security scanning, password cracking, session hijacking, using key loggers, war dialers, vulnerability scanners, causing buffer overflows and having back door accounts is expressly prohibited.
i. Executing any form of network monitoring which will intercept data not intended for the employee's host.
j. Circumventing user authentication or security of any host, network or account.
k. Interfering with or denying service to any user other than the user's host (for example, denial of service attack).
l. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

<u>E-mail and Communications Activities</u>

See *Electronic Mail "E-Mail" Departmental Policy Bulletin 4.135* for further policy guidelines.

a. Sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (e-mail spam).
b. Any form of harassment via e-mail, telephone or paging, whether through language, frequency, or size of messages.
c. Unauthorized use, or forging, of e-mail header information.
d. Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies.
e. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

f. Use of unsolicited e-mail originating from within DPI's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by DPI or connected via DPI's network.

g. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

6. Internet Use

The Department of Public Instruction will use the Internet as an effective, efficient, and timely source of information, method of communication, and vehicle for data collection, information dissemination, and delivery of services to DPI clients and customers. Because of legal, security, and user productivity issues associated with Internet use in the workplace, the DPI has adopted the following policy regarding Internet use by employees. All staff must comply with this policy and the policies for any host machines to which they are granted access.

Internet resources are to be used in a manner consistent with the administrative, informational, instructional, and research objectives of the department. Use of the Internet is primarily intended as a resource for the official work of the department and its mission.

Examples of inappropriate use of resources include, but are not limited to, any use that violates state and/or federal laws, any use that is unethical in nature, distribution of unsolicited advertising, propagation of computer viruses, distribution of chain letters, attempts to make unauthorized entry to another network node, and activities associated with running an employee’s private business or for personal gain. Employees are expected to use discretion in the performance of their duties.

Whenever an employee accesses the Internet, files are automatically written to the local hard drive and to a router at DOA identifying the Internet site accessed and dates and times of the access. SITE ACCESS IS LOGGED and the department conducts periodic reviews for blatant abuse of the system. DPI can block sites.

Incidental personal use is allowed during lunch breaks and before and after work hours. Such use should not interfere or conflict with state use. Personal use will fall under same restrictions as use during working hours. Employees should exercise good judgment regarding the reasonableness of personal Internet use. State-provided resources shall not be used for private or commercial enterprises (see Departmental Policy Bulletin 2.200). Department Internet services may be used for incidental purposes provided that, in addition to the foregoing constraints and conditions, such use does not directly or indirectly interfere with the department's operation of the computing facility or the Internet service; burden the department with noticeable incremental costs; interfere with the obligations to the department; or cause unwarranted interference with the use of the Internet system by others. If division administrators, team directors, team leaders, or leadworker staff become aware that employees are making personal use of the Internet during work hours, the manager or leadworker should immediately inform the employee that such use must cease. If misuse persists, the situation will be brought to the attention of Human Resources staff, who may request a record of the employee’s Internet use from the Technology Services Team. Disciplinary actions may result if it is determined inappropriate use has occurred.

Employees shall respect the privacy of others. Do not seek information about, obtain copies of, or modify electronic information belonging to other users unless explicitly authorized to do so.

Passwords should not be shared with unauthorized users, nor should employees use another individual's password (see Departmental Policy Bulletin 4.100).

Private or confidential information authorized to be exchanged should be in encrypted form.

E. Enforcement

Any user found to have violated this policy may be subject to termination of access to DPI information technology resources or suspension of computing privileges and discipline, up to and including termination.

F. Definitions

Term	**Definition**
FTP	File Transfer Protocol
Packet Spoofing	Falsification of the sending address of a transmission in order to gain illegal entry into a secure system.
Ping	(**P**acket **In**ternet **G**roper) An Internet utility used to determine whether a particular Internet Protocol address is online.
Pinged floods	Ping requests that flood the target computer(s) often causing system crashes.
Ponzi	Distribution of unsolicited advertising, emails, spam, and propagation of computer system with unauthorized network traffic.
Port Scanning	Sending queries to Internet servers in order to obtain information about their services and level of security. Port scanning is sometimes done to determine if a network can be compromised.
Spam	To send copies of the same message to large numbers of newsgroups or users on the Internet. People spam the Internet to advertise products as well as to broadcast some political or social commentary.

Questions concerning this policy should be directed to the Technology Services Team, Division for Libraries, Technology and Community Learning.

Wisconsin Department of Public Instruction
DEPARTMENTAL POLICY BULLETIN
PI-1100 (Rev. 07-09)

Index **4.315**

Subject	Effective Date	Page
CONFIDENTIALITY OF INDIVIDUAL PUPIL DATA AND DATA REDACTION (SCREENING)	**04/01/16**	**1 of 3**

A. Background

This policy was developed to help ensure that state and federal pupil confidentiality laws are not violated in dashboards, reports or data files published and made available publicly by the department or its agents or contractors, that are based on academic performance data, achievement data, or other personally identifiable information related to students or staff in the districts or schools. This policy specifically provides information on data intended for public use and the redaction of that data to protect student privacy.

For information on accessing student identifiable data, or summary data that is not redacted (see Departmental Policy Bulletin 4.300).

B. Legal Considerations

The Federal Education Rights and Privacy Act (FERPA) applies to school districts that receive federal funds from the U.S. Department of Education. The state pupil records law (s. 118.125, Stats.) was created by the Wisconsin legislature and applies to school districts; portions also apply to DPI. Restrictions on the disclosure of income eligibility status for subsidized lunches are provided in federal law under the jurisdiction of the USDA, and compliance is the responsibility of the local school district. The open records law also applies (see Departmental Policy Bulletin 1.130).

The department believes that disclosing an abbreviated public data set adequately protects the confidentiality of individual pupils within the meaning of FERPA and the state pupil records law. A school district may, under local authority, set aside the standards used by DPI in screening the public data set provided to it and choose its own more or less rigorous standard or method of screening and accept the legal risks involved in that decision. Should a school district have any legal questions about disclosing pupil information, the district should be advised to consult with its own legal counsel.

More information on student privacy can be found here: http://wise.dpi.wi.gov/wise_studentdataprivacy.

C. General Redaction Policy

The policy addresses two interests:

1. The confidentiality requirements that exist in state and federal law; and

2. The needs and demands of the community and policy makers for detailed student academic and achievement data by various demographic categories to ensure accountability for the performance of all students and to promote community involvement in school improvement.

The confidentiality provisions of state and federal pupil records laws generally require that any questions about revealing individual pupil identity through the dissemination of information should be resolved in favor of protecting the individual pupil’s identity. Enactment of pupil assessment laws or program changes designed to define and track academic outcomes does not change that principle.

The greatest threat to pupil confidentiality arises when the number of pupils in a particular reported category (gender, ethnicity, socioeconomic class, grade, school, or district) is very small. The smaller the number of children of a particular category, the easier it is to identify individual children. In order to protect pupil confidentiality in these situations, it is necessary to redact personally identifiable information of pupils. The redaction policy provides that, where the numbers of children in a particular category are very small, the information in that category will be redacted from the report in an effort to not suggest an individual pupil's identity.

D. DPI Specific Tools and Examples

1. District and School Report Cards
   a. To protect student privacy, data for groups of fewer than twenty pupils are replaced by asterisks on the public report cards.
   b. NA is used when data are Not Applicable. For example, a district that does not graduate students will have NA listed for graduation results.
   c. Additional details regarding the redaction principles involved in District Report Cards and School Report Cards can be found on Page 2 of the report card itself or in DPI's School Report Card at a Glance documentation which can be found at http://reportcards.dpi.wi.gov/files/oea/pdf/ataglance.pdf

2. WISEdash Public Portal
   a. To protect student privacy, it is necessary to avoid disclosure of confidential information regarding small groups of students so there is not any direct or indirect disclosure of an individual student.
   b. Upon user filtering, the WISEdash Public Portal's aggregated datasets must comply with a strict hierarchy of redaction rules, effectively masking potentially identifiable variables.
   c. More information regarding direct/indirect disclosure and data redaction in the WISEdash Public Portal can be found at http://wise.dpi.wi.gov/wisedash_redaction
   d. Examples of data suppression in the WISEdash Public Portal can be found at http://wise.dpi.wi.gov/wisedash_graphs-nodata
   e. The WISEdash Public displays an asterisk * in a dashboard's data table instead of a number when it's required to mask data with small groups of students. The asterisk * also may appear in a graph's legend by a white box □* .
   f. Definitions of specific redaction terms in the WISEdash Public Portal can be found at http://wise.dpi.wi.gov/wisedash_glossary

3. School District Performance Report (SDPR)—https://apps2.dpi.wi.gov/sdpr/spr.action a. Definitions:
   1) Factor (aka disaggregation factor)—typically demographic attributes such as gender, race/ethnicity, disability status, grade level.
   2) Category—individual values within a factor such as male/female, black/white/Hispanic.
   3) Topic—student behaviors, outcomes, demographic characteristics such as attendance, dropouts, test results, graduation, etc.
   4) Sensitive topic (aka confidential topic)—topics that are deemed to be private information and disclosure must be restricted. Most topics collected by DPI are sensitive.

   b. Suppression Rules: Where a sensitive topic is reported (disaggregated) by a factor:
   1) Perform school-level suppression
      a) (rule 1A) suppress each category where enrollment/count between 1:5
      b) sum suppressed enrollment/count
      c) (rule 1B) if sum between 1:5 then suppress next unsuppressed category with smallest enrollment/count. If tied for smallest, suppress all tied categories

2) Transfer school-level suppression to district-level for single-school categories
   a) count number of schools with each category suppressed at school-level
   b) (rule 2) where count = 1 then suppress same category at district-level
3) Perform district-level suppression
   a) (rule 3A) suppress each category where enrollment/count between 1:5
   b) sum suppressed enrollment/count at district-level
   c) count suppressed categories at district-level
   d) (rule 3B) if sum between 1:5 or (rule 3C) count = 1 then select another category to suppress
   Select the category with the smallest enrollment that:
   i. Has not already been suppressed at the district-level. ii.
   If tied for smallest, suppress all tied categories.

c. Note: “between 1:5” means greater than 0 and less than 6.

d. Note: tiny school rule must be applied before district suppression.

4. Other

a. Teams creating applications that need to display redacted data should take care to ensure that redaction is built into the application. The Division of Libraries and Technology will be able to provide guidance to Application Developers.

b. Teams who publish reports or data files on their own should follow the District/School Report Cards policy or the WISEdash Public Portal policy. Additional detail related to the technical implementation of the WISEdash Public Portal redaction rules are available upon request by submitting a help ticket (http://wise.dpi.wi.gov/help-ticket) and/or contacting the Division of Libraries and Technology.

Wisconsin Department of Public Instruction
DEPARTMENTAL POLICY BULLETIN
PI-1100 (Rev. 07-09)

		Index **4.330**
Subject **POLICIES AND PROCEDURES FOR RESEARCH INVOLVING HUMAN SUBJECTS**	Effective Date **04/01/16**	Page **1 of 4**

A. Introduction

The Department of Public Instruction (DPI) recognizes its ethical and federally mandated responsibility to safeguard the rights and welfare of human subjects in all research undertaken under its sponsorship or on its premises. DPI does not have an internal Institutional Review Board (IRB) but provides for IRB review and approval by entering into IRB Authorization Agreements with outside IRBs approved by the Office for Human Research Protections (OHRP). DPI, working with its designated IRBs (DIRBs), accepts the task of advocate and protector of the community of which they are a part.

For this purpose,

> *Research* means a systematic investigation designed to develop or contribute to generalized knowledge. 45 CFR. § 46.102(d).
>
> *Human subjects* means individuals about whom an investigator obtains: (1) data through intervention or interaction with the individuals, or (2) identifiable private information. 45 CFR. § 46.102(f).

It is the responsibility of the administrators, staff, individual investigators and community members to familiarize themselves with these policies and procedures and the Federal Policy for the Protection of Human Subjects (also known as the “Common Rule”; Title 45 CFR Part 46). Questions about their applicability should be sent in writing to the Human Protections Administrator (HPA) and the Chairperson of the DIRB, or the person indicated in the DIRB’s policies. Interpretation of applicability is the legal right and responsibility solely of the HPA and DIRB respectively.

DPI regards any infringement of these policies and procedures as a serious breach of professional standards. DPI’s support of researchers may depend on strict adherence to policies and procedures regarding DIRB approval.

This document provides information regarding the policies and procedures followed by the DPI and the DIRBs.

B. Ethical Principles Guiding Human Subjects Research

In 1945, information came to light about unethical experiments conducted by Nazi physicians on concentration camp prisoners. Many of these experiments deliberately contributed to or caused the deaths of children and adults. In that same decade, a study in Tuskegee, Alabama funded by the United States government used economically disadvantaged rural African American men to study the untreated course of syphilis. These subjects were not offered effective treatment until long after such treatment was generally available.

These practices, and others, heightened the awareness of the need to protect human subjects and to assure their *informed voluntary consent* to participate in human subjects’ research. The principles that underlie human subject protections today are found in three main documents—the Nuremberg Code, The Declaration of Helsinki, and The Belmont Report. In 1974 the National Research Act (Pub. L. 93-348) was signed into law and the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research was established. In addition, academic disciplines, primarily through their professional organizations, have developed codes of ethical conduct regarding the involvement of practitioners and researchers with human subjects. The work of the National Commission is summarized in The Belmont Report[1]. This document identifies three basic ethical principles that should guide research involving human subjects. These principles are *respect of persons, beneficence, and justice*; and should serve as a guide to researchers in designing research protocols, strategies, and procedures at and for the DPI, and to the evaluations of proposals made by the DIRBs.

1. Respect of Persons
   The principle of respect of persons requires that researchers should obtain the informed consent of all human subjects invited to participate in research. In order to respect subject autonomy, the consent process should include giving subjects full and comprehensible information about the research and providing clear assurance that participation is voluntary. Subjects must be given explicit assurances regarding the voluntary nature of their participation in terms that are easy to understand and do not place the subject under duress.

   Investigators should spell out in the language of lay persons any foreseeable physical, psychological, economic, and social risks which participation in the research might bring to the subject immediately or in the future. This should be done even if the risks are described to the subject as insubstantial.

   In addition, respect means honoring the privacy of individuals and maintaining confidentiality. Respect for minors and mentally disabled persons requires taking extra precautions to protect those individuals who are immature or incapacitated, perhaps even to the extent of excluding them from participation in certain research studies. The extent of protection depends on the risks and benefits of the research to the participants.

2. Beneficence
   The principle of beneficence requires that researchers maximize the potential benefits to subjects and minimize the potential risks of harm. Benefits to the subjects, which may be in the form of generalized knowledge gained from the research, should always outweigh the risks. Finally, if there are any risks resulting from participation in the research, then there must be benefits, either to the subject, humanity or society in general.

3. Justice
   The principle of justice requires that the selection of human subjects should be fair and equitable, and that the risks and benefits of research should be distributed among subjects in a fair and equitable manner. Particular concern should be addressed to subjects whose personal status or condition (such as children, prisoners, patients, and impoverished persons) places them in a vulnerable or dependent status. Principal Investigators (PIs) should be aware of the fact that circumstances sometimes make the inclusion or exclusion of these particularly vulnerable populations unfair.

   Investigators should select subjects based on those factors that most effectively and soundly address the research problem. PIs should avoid selecting subjects based on easy availability if that availability is the result of recent or continuing racial, sexual, religious, or other forms of illegal discrimination. Also,

[1] Full text of The Belmont Report may be found at http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.htm.

investigators must be mindful of the fact that supervisors, using subordinates for research, risk the appearance of soliciting cooperation with unfair pressure.

In many areas of research, data extracted from human subjects can be of great interest to the subjects. Unfortunately, it can be of equal interest to those who might use it in ways that are not in the subjects' best interests. Therefore, it is incumbent upon investigators that they treat the data from subjects as confidential. In contrast, in dealing with subjects, a PI should consider the data as shared information, rather than the investigator's private property, and view the subjects more as partners in research than as mere vessels of data.

C. To Whom Do These Guidelines Apply?

These guidelines apply to all research that:

- is covered by the Common Rule;
- involves human subjects;
- is not exempt under the Common Rule; and
- is carried out by DPI staff, administrators, partners, contractors, companies, government units, or other individuals or units affiliated with DPI or acting in capacities defined by their relationship with DPI.

Included among specific activities to which these policies and procedures apply are all federally funded or sponsored biological, behavioral, psychological and sociological investigations designed to elicit non-public information about individuals or groups.

Excluded from this definition are activities:

- whose sole purpose is instructional; and
- that are directly related to routine DPI program development or evaluation.

D. Institutional Review and Approval

The principal mechanism by which DPI carries out its federally mandated responsibility to oversee research involving human subjects is the formal DIRB review. All federally supported non-exempt human subjects research, which is subject to the Common Rule, must therefore be reviewed and approved by a DIRB.

E. Continuing Review

Federal regulations and good sense dictate that the DIRB review research projects at timely intervals to ensure that no major change in protocols has occurred since approval was first granted. As a result, initial DIRB approval of research projects will be granted for a maximum period of twelve months from the date of review that appears on the approval letter sent to the PI.

Human subjects may be placed at risk not only when data are being gathered but also when results are published. Issues of confidentiality are most likely to arise during dissemination or publication. DIRB approval must therefore be renewed as indicated above, until no further related activity is contemplated.

F. DIRB Oversight

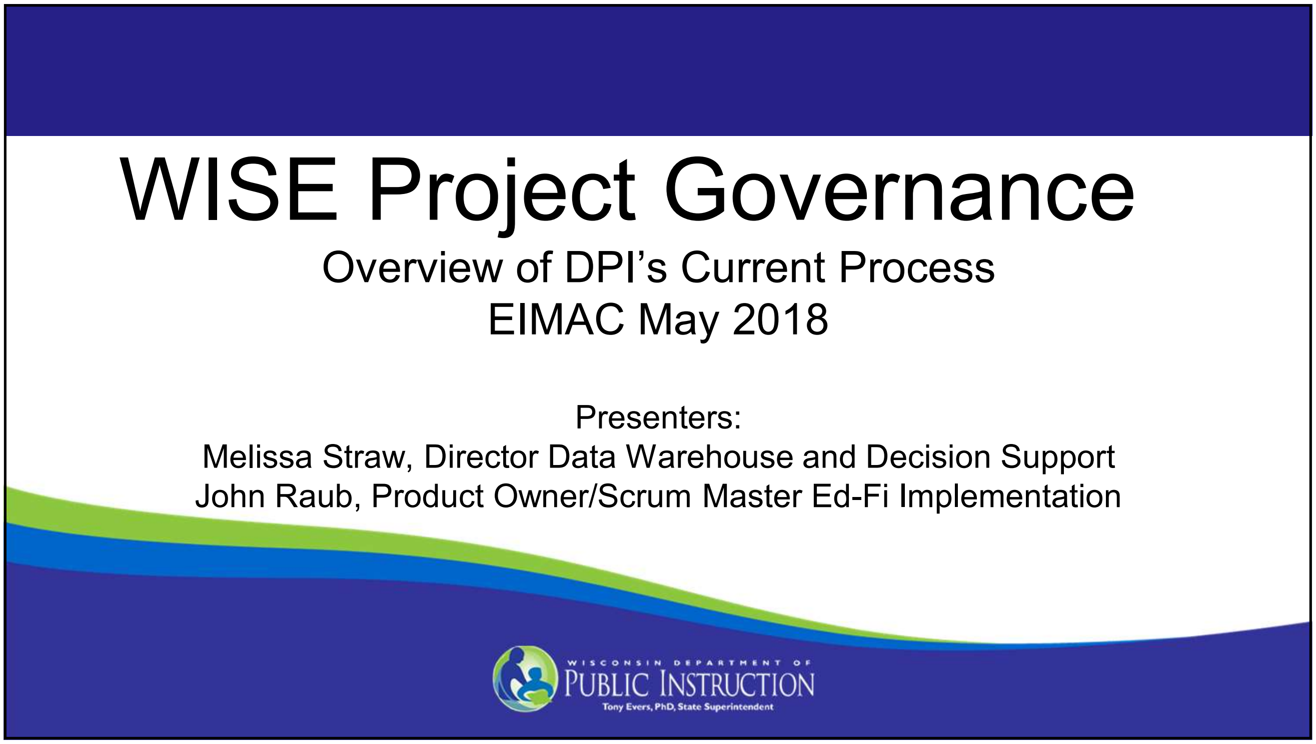
Oversight of the work of the DIRBs is conducted by the HPA. Concerns, questions, or complaints regarding the work of a DIRB in carrying out its mandated responsibilities regarding human subjects review in research should be directed to:

Human Protections Administrator
Wisconsin Department of Public Instruction
125 South Webster Street
PO Box 7841
Madison, WI 53707-7841

G. Procedures for Prompt Reporting

In order to ensure compliance with the requirements of DPI's *Policies and Procedures for Research Involving Human Subjects* and the requirements of the federal Office of Human Research Protections, it shall be the responsibility of all administrators, staff, individual investigators and community members familiar with any research undertaken pursuant to the *Policies and Procedures for Research Involving Human Subjects*, to promptly report to the HPA, the Chair of the DIRB (or DIRB-designated individual), the head of any U.S. federal department or agency conducting or supporting the research (or designee), and the federal Office of Human Research Protections, any:

1. unanticipated problems involving risks to subjects or others;
2. serious or continuing noncompliance with the applicable U.S. federal regulations or the requirements or determinations of the DIRB(s); and
3. suspension or termination of any DIRB(s) approval.

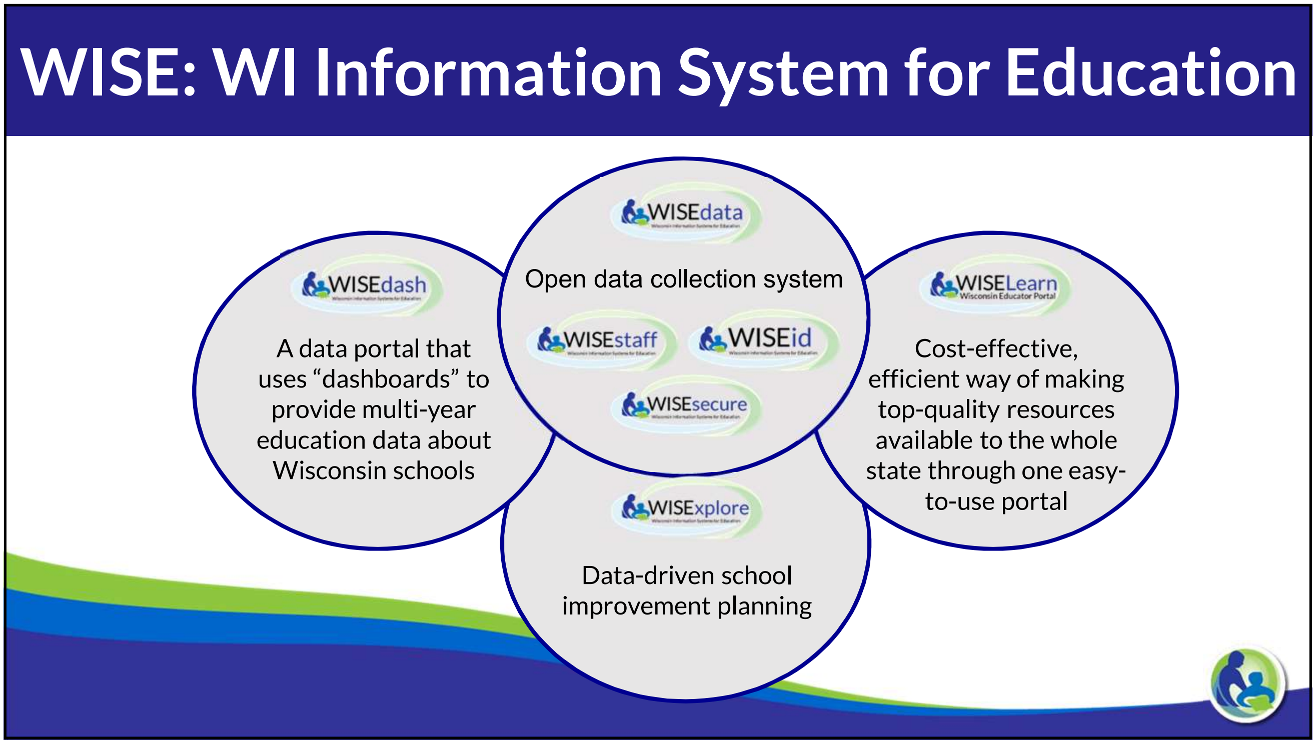


WISE Project Governance

Overview of DPI's Current Process
EIMAC May 2018

Presenters:
Melissa Straw, Director Data Warehouse and Decision Support
John Raub, Product Owner/Scrum Master Ed-Fi Implementation

WISCONSIN DEPARTMENT OF PUBLIC INSTRUCTION
Tony Evers, PhD, State Superintendent



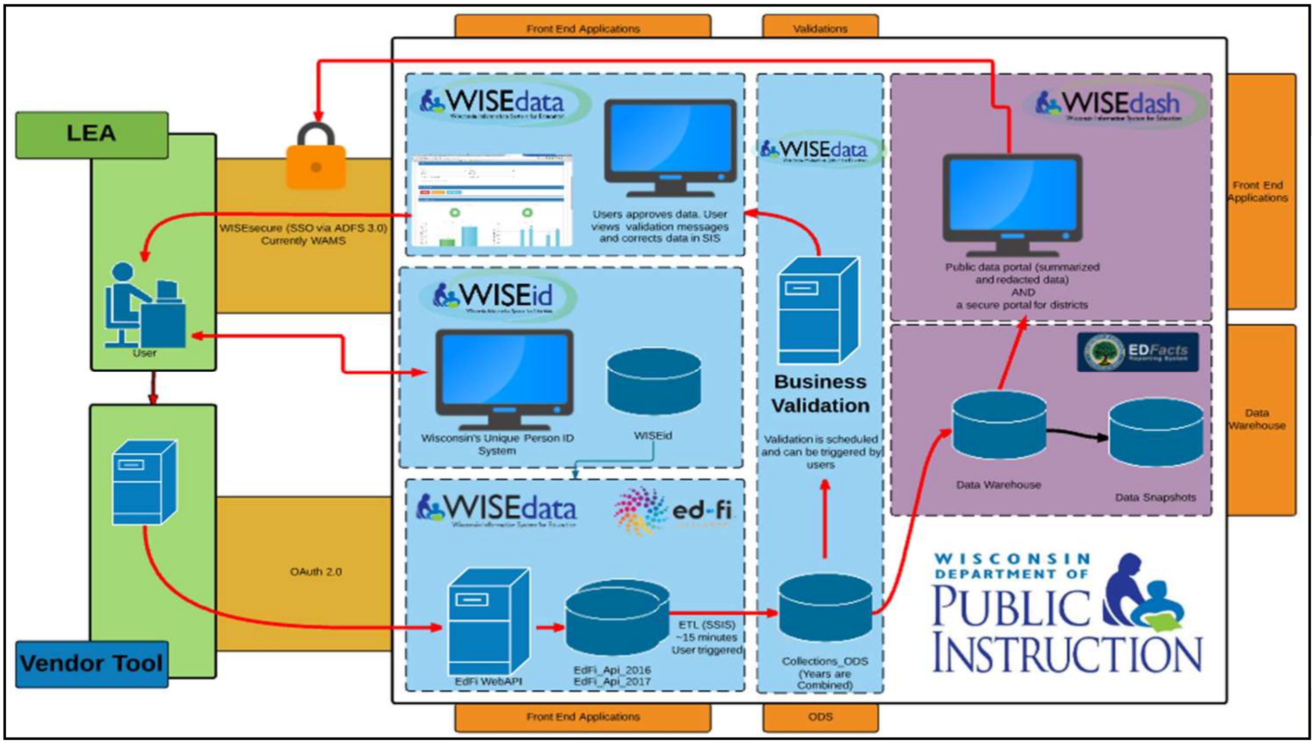
WISE: WI Information System for Education

WISEdata
Open data collection system
WISEstaff
WISEid
WISEsecure

WISEdash
A data portal that uses "dashboards" to provide multi-year education data about Wisconsin schools

WISELearn
Wisconsin Educator Portal
Cost-effective, efficient way of making top-quality resources available to the whole state through one easy-to-use portal

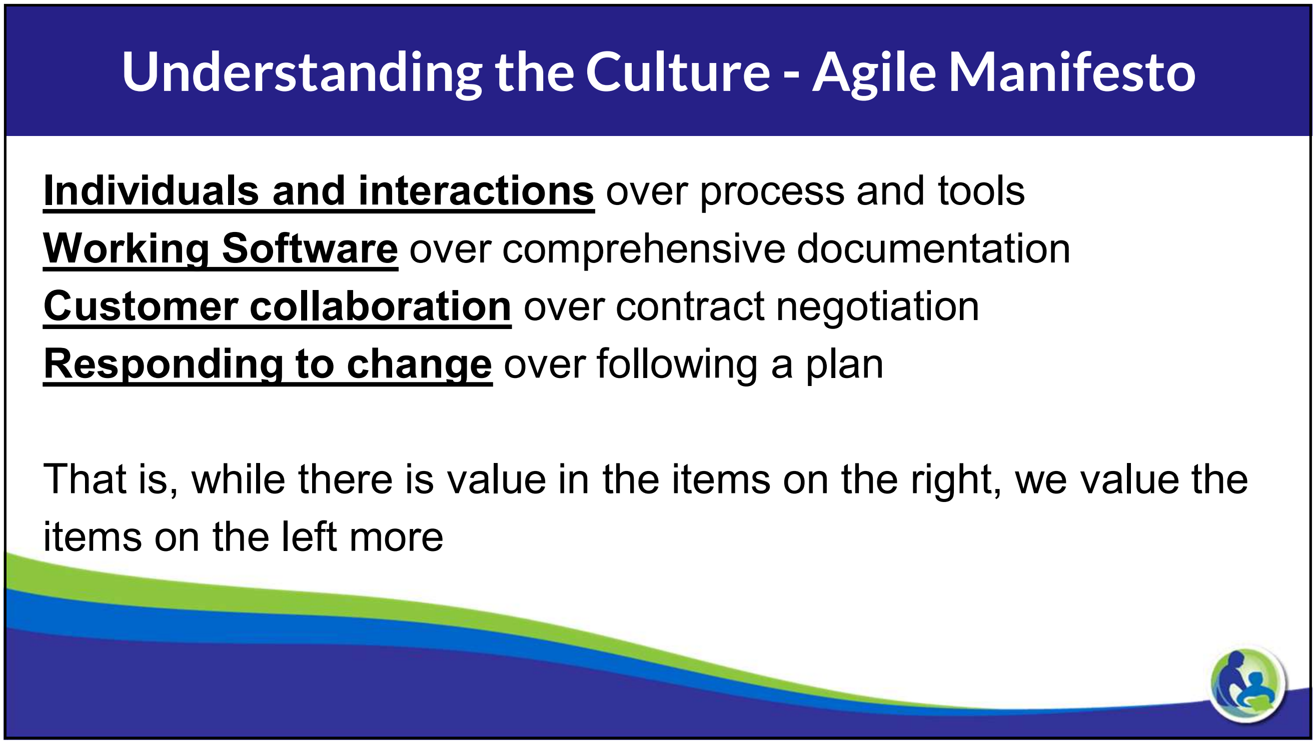
WISExplore
Data-driven school improvement planning



WISE Project Governance

- Scrum Teams
- WISE Leadership Team
- WISE Steering Committee
- IT Project Request Process and Prioritization

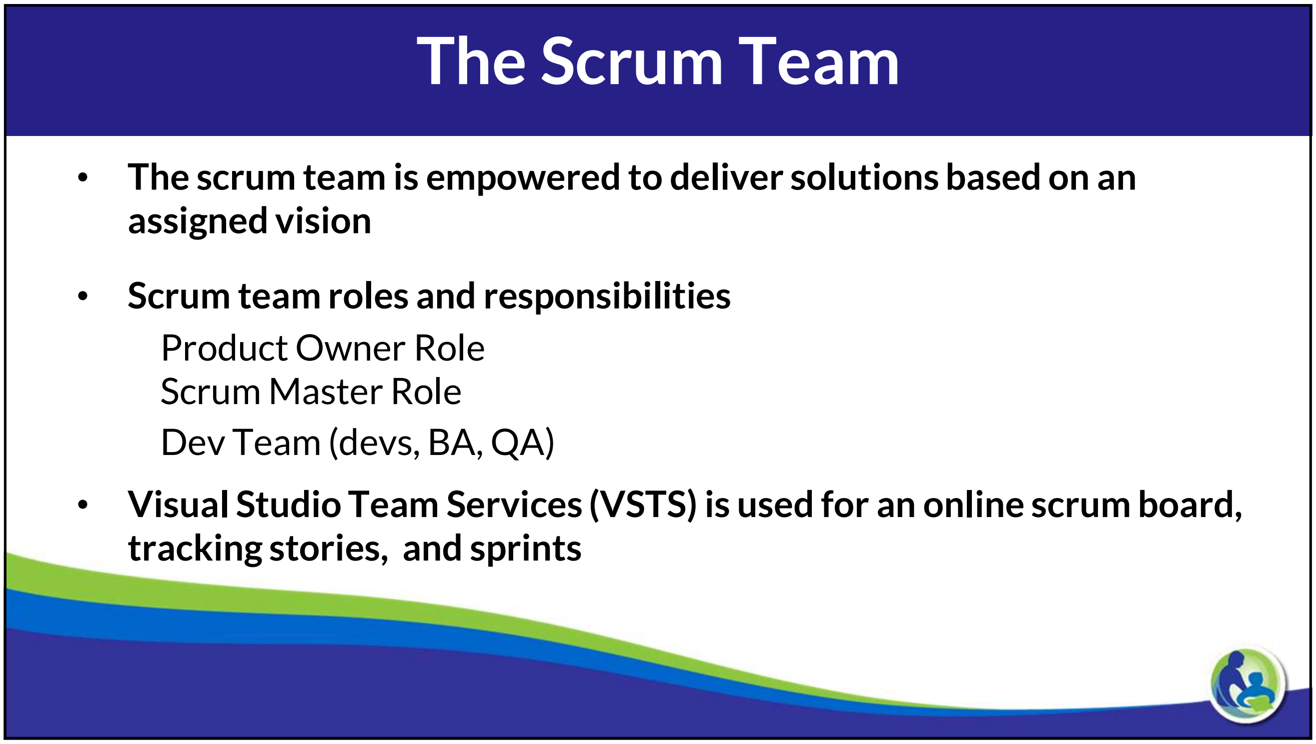
Scrum Teams



Understanding the Culture - Agile Manifesto

Individuals and interactions over process and tools
Working Software over comprehensive documentation
Customer collaboration over contract negotiation
Responding to change over following a plan

That is, while there is value in the items on the right, we value the items on the left more

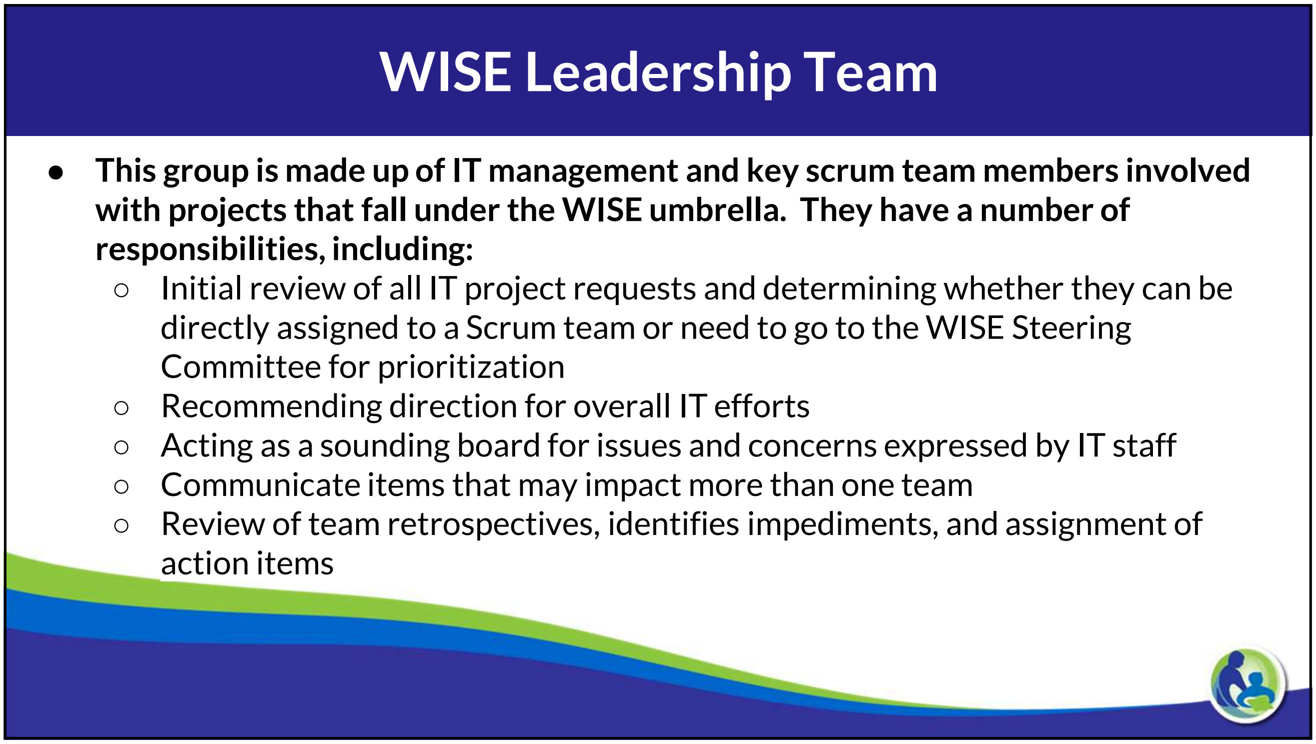


The Scrum Team

- **The scrum team is empowered to deliver solutions based on an assigned vision**
- **Scrum team roles and responsibilities**

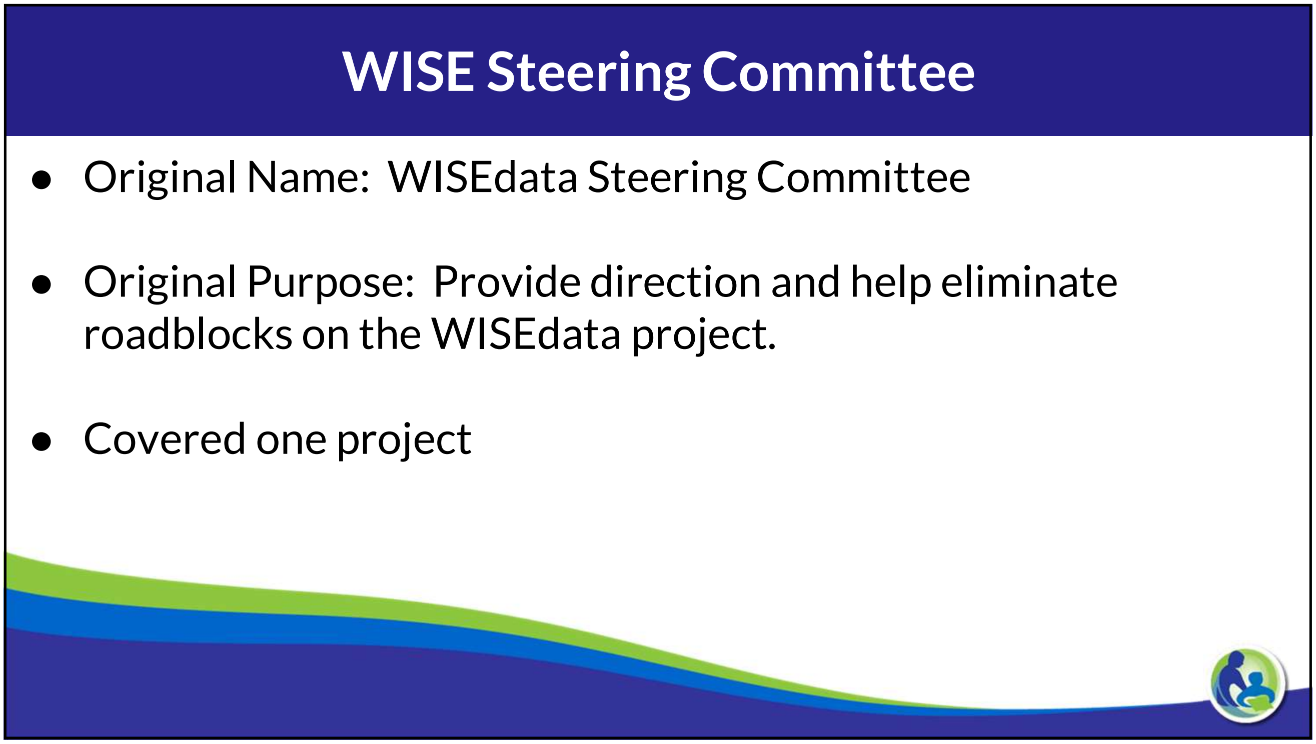
  Product Owner Role
  Scrum Master Role
  Dev Team (devs, BA, QA)
- **Visual Studio Team Services (VSTS) is used for an online scrum board, tracking stories, and sprints**

WISE Leadership Team and WISE Steering Committee



WISE Leadership Team

- **This group is made up of IT management and key scrum team members involved with projects that fall under the WISE umbrella. They have a number of responsibilities, including:**
  - Initial review of all IT project requests and determining whether they can be directly assigned to a Scrum team or need to go to the WISE Steering Committee for prioritization
  - Recommending direction for overall IT efforts
  - Acting as a sounding board for issues and concerns expressed by IT staff
  - Communicate items that may impact more than one team
  - Review of team retrospectives, identifies impediments, and assignment of action items



WISE Steering Committee

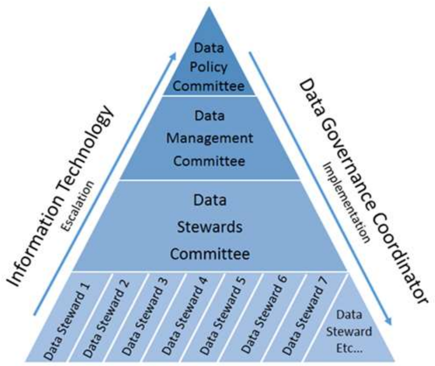
- Original Name: WISEdata Steering Committee
- Original Purpose: Provide direction and help eliminate roadblocks on the WISEdata project.
- Covered one project

WISE Steering Committee

- Updated Name: WISE Steering Committee
- Updated Purpose: Discuss and collaborate on IT projects that fall under the WISE umbrella including additional collections and data elements to be brought into the WISEdata system.
- Cross agency group that covers all of WISE.

- Prioritizes project work which is critical when program areas are competing for scrum team/staff time. Informs roadmap.
  - Goal: Transparency, Criterion-driven consensus-based decision making

Data Governance @ DPI



The Data Policy Committee is responsible for setting key policies for the agency and carrying out the legal and policy directives of the agency's leadership. The DPC is comprised of DPI Directors from the divisions who regularly interact with data.

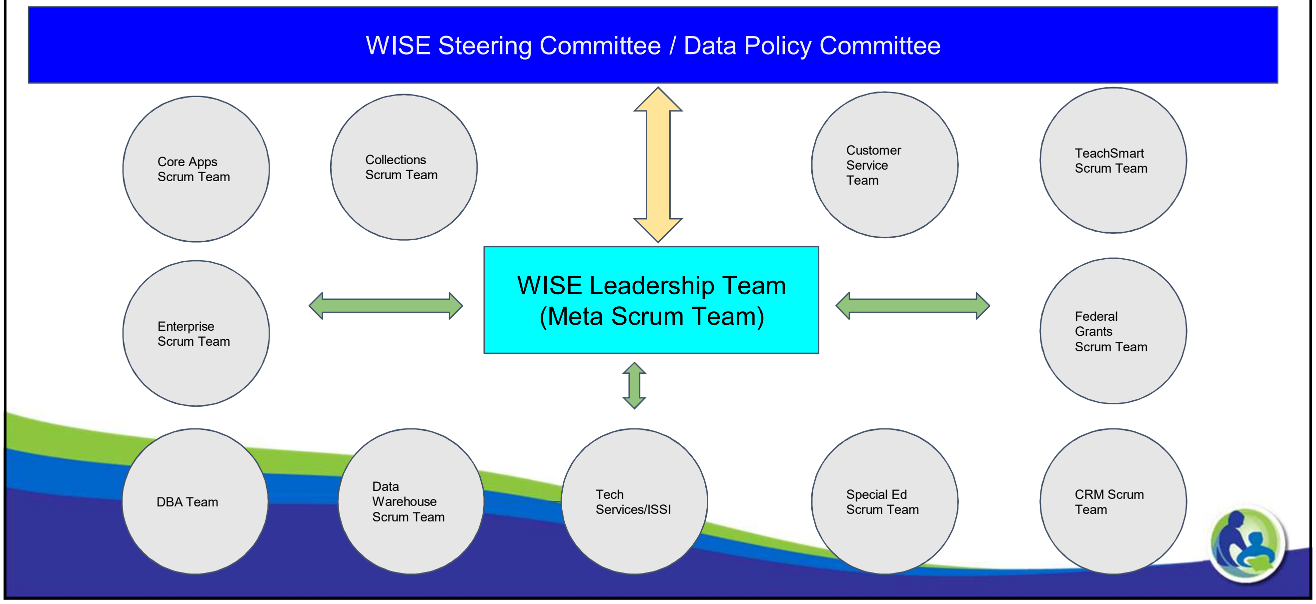
Instead of a separate committee, data policy decisions and tasks will be incorporated into the WISE Steering Committee.

Committee meetings monthly for an hour, some follow-up and team conversations likely

Data Governance

- The WISE Steering committee also represents the policy tier of DPI’s data governance hierarchy
- Additional responsibilities include:
  - Responsible for reviewing and approving confidential data requests
  - Establishing and staffing the Data Management Committee as well as the Data Steward Committee
  - Reviewing and providing feedback on policies before they are submitted through the DPI process for policy approval

DPI WISE Project Structure



WISE Steering Committee / Data Policy Committee

WISE Leadership Team (Meta Scrum Team)

Core Apps Scrum Team

Collections Scrum Team

Customer Service Team

TeachSmart Scrum Team

Enterprise Scrum Team

Federal Grants Scrum Team

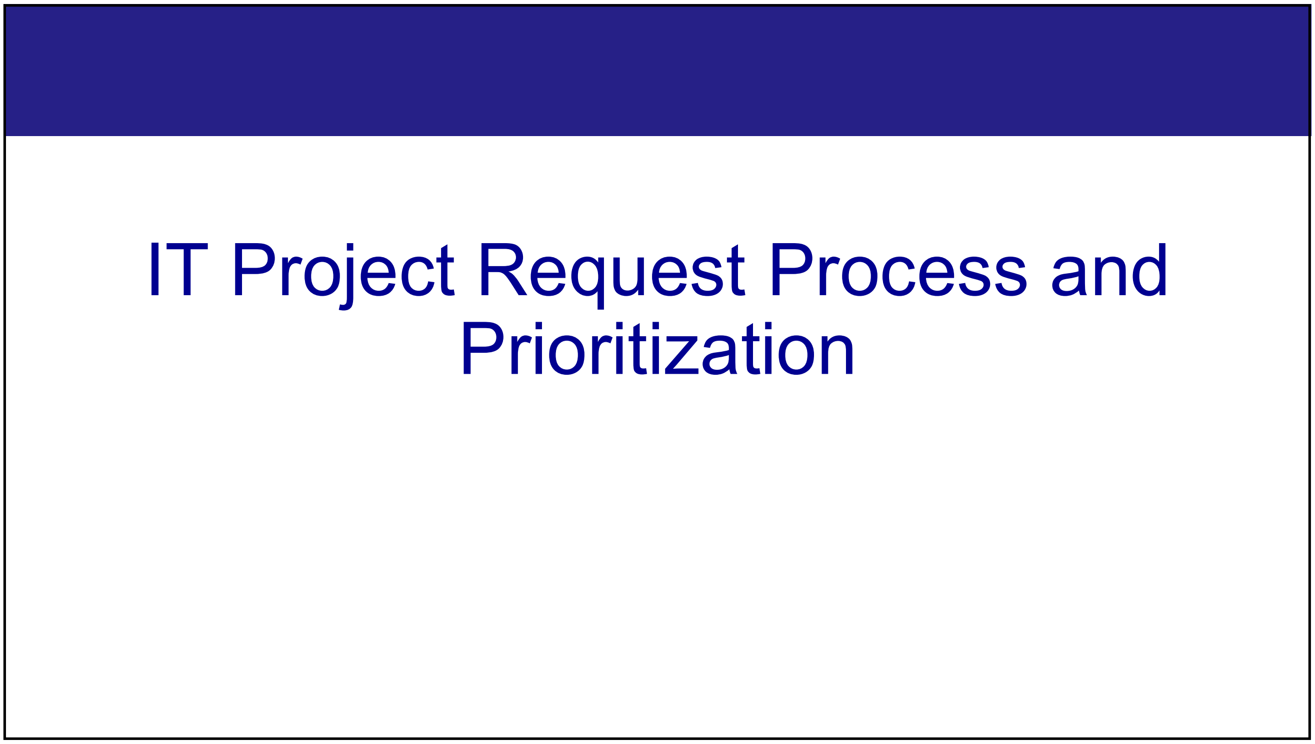
DBA Team

Data Warehouse Scrum Team

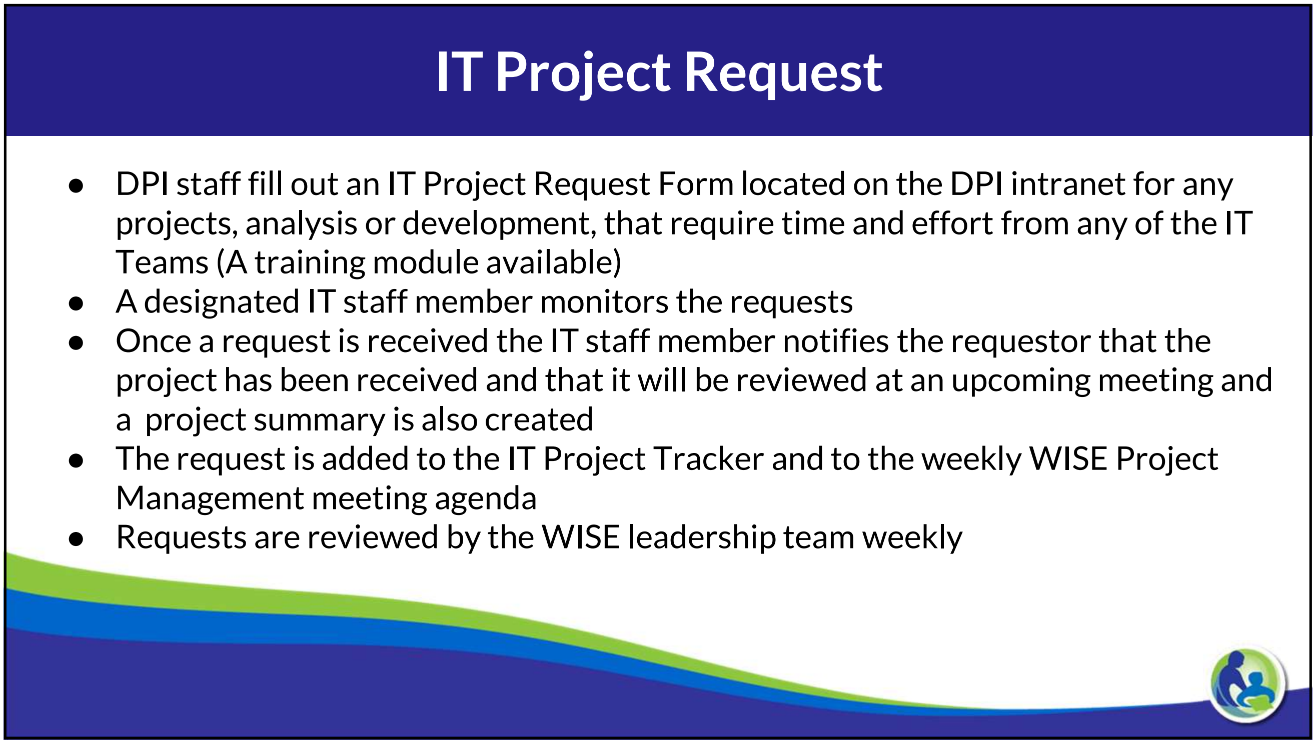
Tech Services/ISSI

Special Ed Scrum Team

CRM Scrum Team

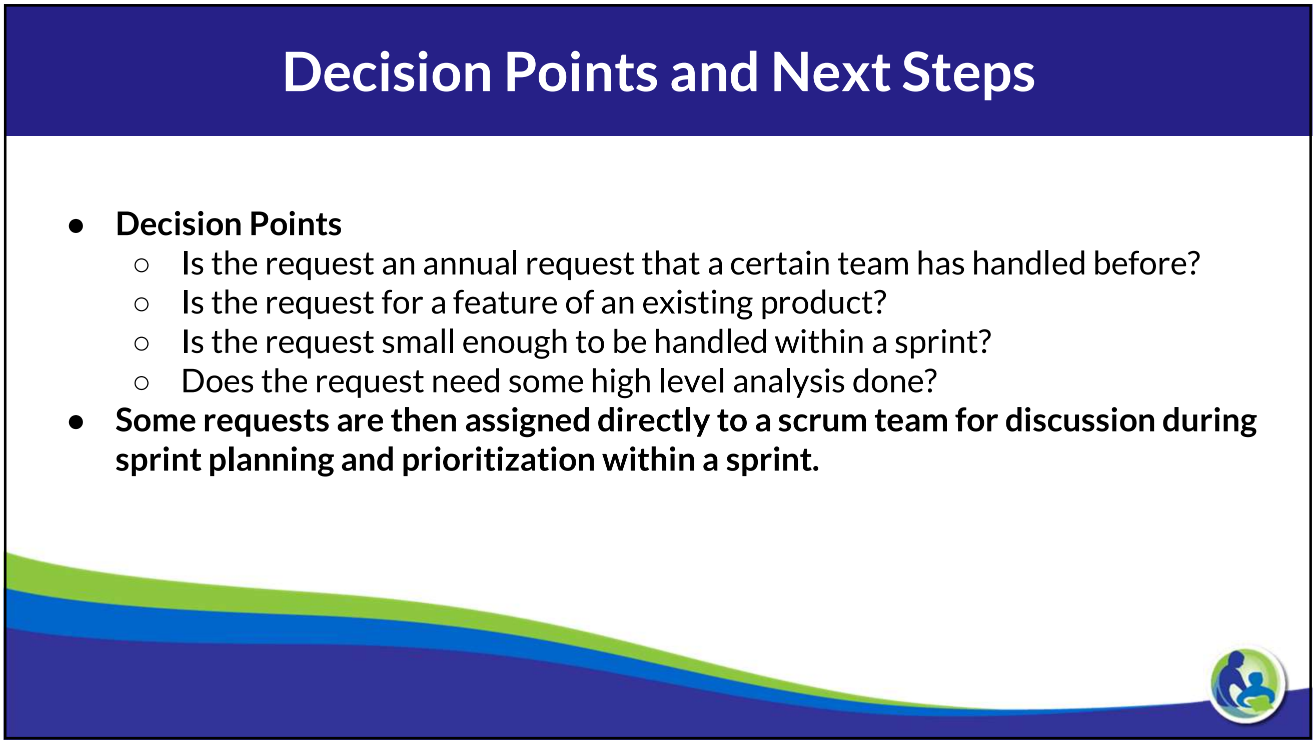


IT Project Request Process and Prioritization



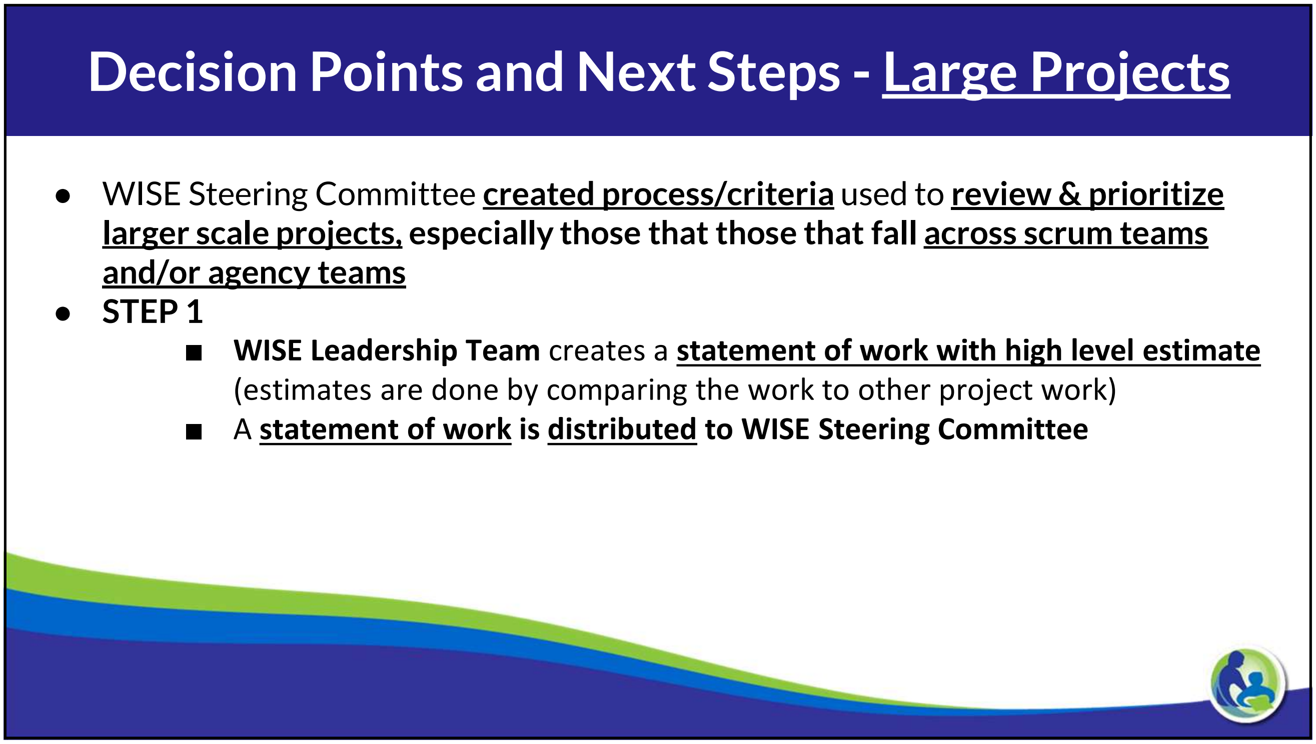
IT Project Request

- DPI staff fill out an IT Project Request Form located on the DPI intranet for any projects, analysis or development, that require time and effort from any of the IT Teams (A training module available)
- A designated IT staff member monitors the requests
- Once a request is received the IT staff member notifies the requestor that the project has been received and that it will be reviewed at an upcoming meeting and a project summary is also created
- The request is added to the IT Project Tracker and to the weekly WISE Project Management meeting agenda
- Requests are reviewed by the WISE leadership team weekly



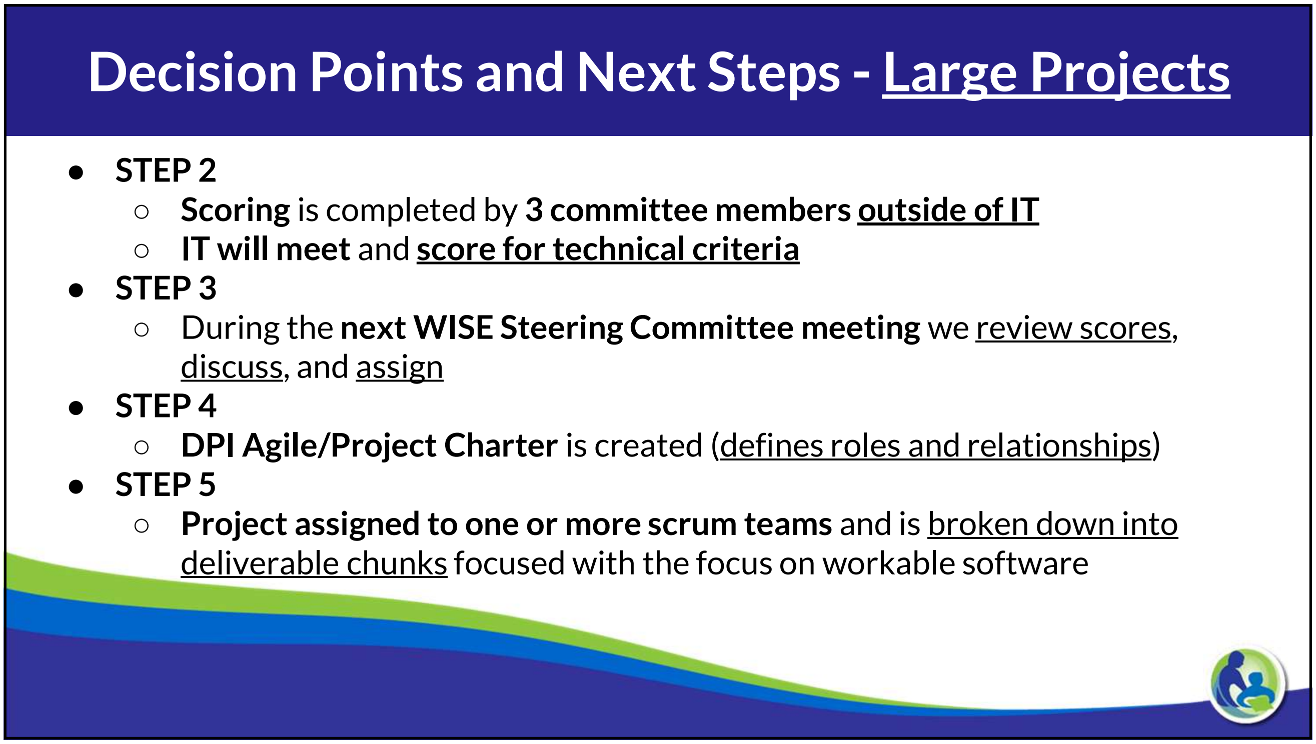
Decision Points and Next Steps

- **Decision Points**
  - Is the request an annual request that a certain team has handled before?
  - Is the request for a feature of an existing product?
  - Is the request small enough to be handled within a sprint?
  - Does the request need some high level analysis done?
- **Some requests are then assigned directly to a scrum team for discussion during sprint planning and prioritization within a sprint.**



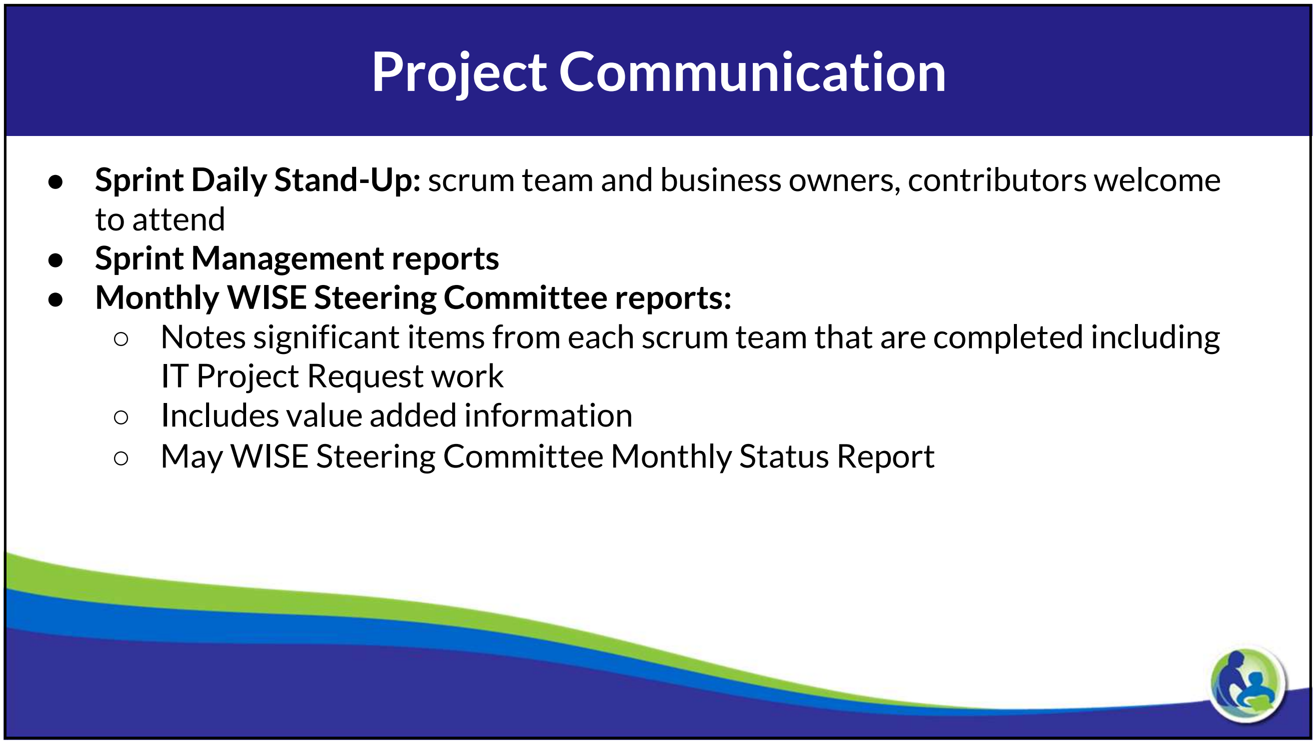
Decision Points and Next Steps - Large Projects

- WISE Steering Committee **created process/criteria** used to **review & prioritize larger scale projects, especially those that those that fall across scrum teams and/or agency teams**
- **STEP 1**
  - **WISE Leadership Team** creates a **statement of work with high level estimate** (estimates are done by comparing the work to other project work)
  - A **statement of work is distributed to WISE Steering Committee**



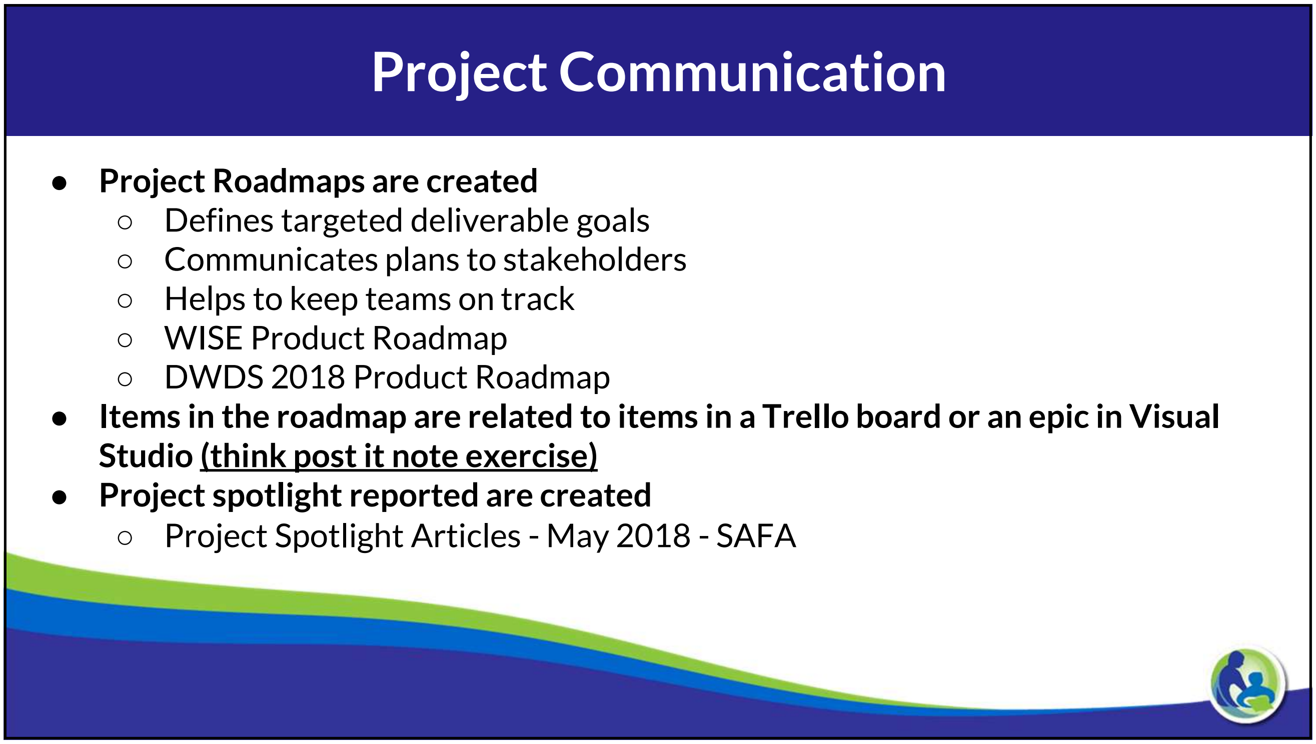
Decision Points and Next Steps - Large Projects

- STEP 2
  - **Scoring** is completed by **3 committee members outside of IT**
  - **IT will meet** and **score for technical criteria**
- STEP 3
  - During the **next WISE Steering Committee meeting** we review scores, discuss, and assign
- STEP 4
  - **DPI Agile/Project Charter** is created (defines roles and relationships)
- STEP 5
  - **Project assigned to one or more scrum teams** and is broken down into deliverable chunks focused with the focus on workable software



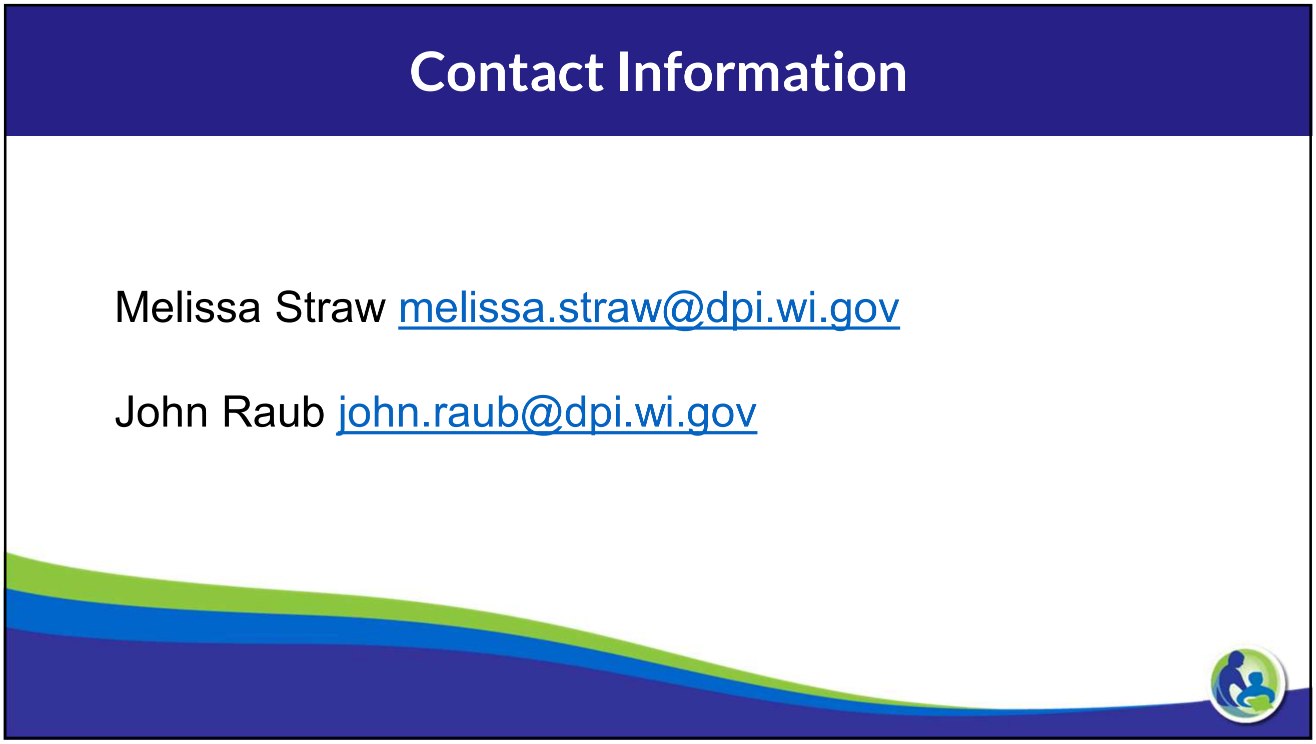
Project Communication

- **Sprint Daily Stand-Up:** scrum team and business owners, contributors welcome to attend
- **Sprint Management reports**
- **Monthly WISE Steering Committee reports:**
  - Notes significant items from each scrum team that are completed including IT Project Request work
  - Includes value added information
  - May WISE Steering Committee Monthly Status Report



Project Communication

- **Project Roadmaps are created**
  - Defines targeted deliverable goals
  - Communicates plans to stakeholders
  - Helps to keep teams on track
  - WISE Product Roadmap
  - DWDS 2018 Product Roadmap
- **Items in the roadmap are related to items in a Trello board or an epic in Visual Studio (think post it note exercise)**
- **Project spotlight reported are created**
  - Project Spotlight Articles - May 2018 - SAFA



Contact Information

Melissa Straw melissa.straw@dpi.wi.gov

John Raub john.raub@dpi.wi.gov

DPI Internal Data Access Request Process

The DPI Internal Data Access Request Process was developed for DPI staff to request access to data in an application and/or database once a legitimate need for access has been determined. This is a request that is above and beyond an onboarding request for new employees and will also be used for current employees. This process results in documentation of the request, approval, and completion of the request. Confidentiality training should be completed before submitting the request regardless if the request is for student or staff data. If Student level data access is needed, be prepared to provide the reason why you need Student Level data in the request.

I. Workflow for Production Application Request

a. A WAMS ID is required for application access. If you do not have a WAMS id, go to https://on.wisconsin.gov/WAMS/home and create a WAMS ID through the “Self-Registration” Process. Use your DPI email when creating your ID.

b. The Director and staff member should review the roles in Appendix A determine which role is needed to complete job related tasks.

c. Contact the Product Owner listed with any questions prior to submitting the request.

   i. For WISEgrants it is required that you contact the Product Owner prior to submitting the request. They will need to work with you to determine the application level role you will need. This role will need to be entered into the description of the request.

   ii. For Power BI access requests, once the program area Director approves the request it will be routed to Melissa Straw to review and then assign to ISSI for setup.

d. Next, initiate the request by creating a Data Access Request in Footprints.

e. The ticket will be routed first to the Director of the program area selected for approval.

f. After it is approved, the ticket will be routed to the IT Customer Services Team (CST) to set the user up with the requested access using ASM. For Special Ed applications it will route to the Special Ed team instead. It will only be assigned once fully approved. ASM automatically sends emails when access is granted. Ticket will be closed. If the request is not approved it will be closed and an email will be sent to the requestor explaining the reason.

II. Workflow for Production SQL Database Request (NEW)

In most cases users do NOT need direct access to query a database. If this type of access is needed there are different steps that need to happen to determine the appropriate access, to create the necessary roles and AD groups if needed, and to train the requestor on how to query the data they need. In these cases we need to rely on the expertise of the IT Product Owners to help determine the right path to take for a direct database request. (The IT Product Owner for different Topic Areas can be determined from the Database Topics and Owners table in Appendix A.)

a. The staff member who will be requesting the access and their Director should review the roles in Appendix A determine which role is needed to complete job related tasks.

b. Contact the Product Owner listed with any questions prior to submitting the request.

c. Next, initiate the request by creating a Data Access Request in Footprints.

d. The ticket will be routed first to the Database Approver/Product Owner. An email will be sent letting them know that a new request was submitted and that they need to review and fill in the field with the appropriate AD Group.

   i. Product Owner Responsibilities

      1. The Product Owner or IT Director should work with the DBAs to document and understand the database roles and which AD groups link up to the roles.
      2. The Product Owner will add the AD Group into the database role field. For Oracle add the role.

e. Once the database role is filled out the ticket will then go to the Director of the program area selected for approval.

f. After it is approved, the ticket will be routed to ISSI. It will only be assigned once fully approved. Ticket will be closed and requestor notified when access has been granted by adding the requestor's AD account to the AD group(s) identified in step d.i.2. above. If the request is not approved it will be closed and an email will be sent to the requestor explaining the reason.

III. Workflow for Production Oracle Database Request

a. Same as above except after it is approved, the ticket will be routed to the Oracle DBA so that the requestor can be added to the database security. Ticket will be closed and requestor notified when access has been granted.

IV. Workflow for non-Prod Environments

a. Use Case 1 (Direct Database Access to a Dev Database): A new team member starts on a dev team and needs direct database access to non-prod. For this use case we don't need a separate request. Just by the nature of their role they are approved for development access. The manager of the dev team can request this access via a story on the ISSI scrum board. The manager should work with the product owner listed below ahead of time and include the specific AD group in the request.

b. Use Case 2 (Access to an Application on a Test/UAT server): A program area user, who already is approved for prod app access, needs test or UAT for testing. Because they are approved for prod access they can be setup with non-prod. If they do not have prod access a ticket will need to be submitted and either/or/both prod and UAT access will be granted via the same ticket. Please detail out in the ticket which environments are needed.

c. Use Case 3 (Access to Test/UAT databases for non-development teams): TBD

d. Use Case 4 (Vendor UAT access): Use FootPrints form https://dpi.wi.gov/wisedata/vendors/contact-us which will send Perry and Derew an e-mail notification to alert us to vendor UAT requests.

V. Workflow for App User Account Access for Prod and Non-Prod

a. Contact the scrum team and the scrum team will determine the appropriate access and create a DBA story. Ex: IEP PTP application needing access to the view created in the data warehouse.

VI. Workflow for Creating an Access Request for an Internal/External User without a DPI User ID

a. With prior Director approval, a DPI staff member of the team who is sponsoring this access should login and submit an Internal Data Access Request for the approved individual(s) [User(s)].
b. Before moving on with the request, make sure the User for whom you are submitting the request has reviewed all the resources from FRED under "What to do before you request data access".
c. Also, have the user complete the Data Access Request for Training / Limited Use form.
d. In the form the Contact Information fields are loaded with the Active Directory information associated with your User ID. Because you, as the Program Area who is sponsoring this request, are completing the request for an external user.
    i. If you are doing this request for multiple users keep your information in all fields.
    ii. If you are doing this request for an individual users update all fields to indicate the User's Name, Email Address, Phone Number, and the location where the user will be accessing the DPI system from.
    iii. Enter the legitimate educational need to why you are requesting for this user to gain data access in the "Description" field. If your request is for individual student level data, include specific reasons why student level data access is needed. Also enter any additional information i.e. for assistance to install a database tool or supporting information for the security data access request.
    iv. Attach the form which the User completed under this section, and any additional supporting information for the security data access request.
    v. Optionally, in the Notifications section, enter an individual's email address who you want notified this request was made in the "Address" field. It is suggested to enter the User's email address.

VII. Reports and Auditing

a. A report will be made available so that PO's can review the application and database access.
    i. Footprints report for requests:

1. Security reports are shared and available Footprints. See YYYY Security Requests (Customer) for detailed access requests by year. If a team would like a report created for their specific applications please email the help desk.

ii. ASM report for application access:

iii. Google sheet for database access:

VIII. Adding New Applications or Roles, Updating Roles, or Updating Database Topics

a. For any application additions or changes, the Product Owner or IT Director should identify any new roles that are needed or any changes to roles.

i. The PO should create a story in the Enterprise backlog to add new apps/roles to ASM. If internal, the Definition Of Done in the story should include emailing the help desk to update the selections in Footprints. Last update the Roles and Descriptions below.

b. For any SQL database security additions or changes, the Product Owner or IT Director should work with the DBAs to determine if access permissions for existing AD groups need to be expanded or if new AD groups are needed.

i. To start, the PO or IT Director should create a user story on the DBA board to initiate the conversations with the DBAs.

ii. The PO or IT Director, DBA, and possibly others will work together to finalize the requirements for updating or expanding security permissions on the database for a particular AD group and/or defining security permissions on the database for a new AD group.

iii. identify any new roles that are needed or any changes to roles.

iv. If a new AD group is needed, the DBA will create a story on the ISSI board for the AD group to be created.

v. Once created the AD group should be linked with the database security.

c. For any Oracle database additions or changes, the Product Owner or IT Director should work with the DBA to determine if access permissions for existing security on the database needs to be expanded or if new security needs to be defined and created.

Appendix A: Role Descriptions

Additional scrum team info

Database Topics and Owners

Team Responsible for Setup: ISSI for SQL Server, DBAs for Oracle

Topic Area	Database	IT Team Owner	Product Owner	Special Considerations
AIDS	SQL	Enterprise	Jesila Jinnah	
Contact Labels Application	Oracle	Enterprise	Kari Tenley	Access to this application is managed through Oracle database security. That is why it appears in this list instead of the Application List. Also, email helpdesk@dpi.wi.gov to have ContactLabels-SC (yellow envelope icon) added to your desktop.
DPI Staff Directory Database	SQL	Core Apps	Josh Roy	
DWDS Student Matching	SQL	DWDS	Melissa Straw	Access to this application is managed through AD groups NOT ASM. That is why it appears in this list instead of the Application List. Note for Product Owner: Use G-DWDSStudentMatch.
DPI Master	SQL	Enterprise	Jesila Jinnah	Enterprise database on SQL Server
ECIDS	SQL	DWDS	Melissa Straw	
ELO	SQL	TEPDL	Philip Crawford	
Email Application	Oracle	Enterprise	Kari Tenley	Access to this application is managed through Oracle database security. That is why it appears in this list instead of the Application List.
Enterprise	Oracle	Enterprise	Jesila Jinnah	
GED	SQL	Core Apps	Josh Roy	
TEPDL DMS (Sharepoint)	SQL	TEPDL	Philip Crawford	Access to Sharepoint is managed through AD groups NOT ASM. That is why it appears in this list instead of the Application List.
SSRS	SQL	DWDS	Vinod Dhanabalan	Access to SSRS is managed through AD groups NOT ASM. That is why it appears in this list

				instead of the Application List.
WISEdash	SQL	DWDS	Melissa Straw	
WISEdata	SQL	Collections	John Raub	
WISEid	SQL	Core Apps	Josh Roy	
WISEgrants	SQL	Grants	Matt Baier & Rachel Zellmer	
WISEsecure	SQL	Enterprise	Jesila Jinnah	
WISEstaff	SQL	Core Apps	Josh Roy	
WISE DQ Database	SQL	DWDS	Melissa Straw	This database houses data to create data quality metrics for different WISE applications using tools such as Power BI. Examples of data in this database includes: L2 error counts, acknowledgements, CRM ticket counts, etc.

Applications and DPI Roles

Team Responsible for Setup: CST for all Applications except Special Ed

Application	In ASM?	WAMS ID Needed?	Role	Role Desc	Team	Main Contact	Special Considerations
Aids Banking Admin	YES	YES	BusinessOfficeApproval	Approves/Denies W9 info and banking info	Enterprise	Jesila Jinnah	
			DOALGIPAdmin	Assigns/Approves LGIP number			
			ReadNonConfidentialData	Can view the AB Admin data			
Application Security Manager (ASM)	N/A	YES	College and Career Ready – Manager Role Admin	Assigns user roles to the CCR application for DPI users.	CST	Jeff Perry & Derew Osborne	In most cases CST (Jeff and Derew) will be the only people with role admin privleges for an application to assign access to internal DPI users. For Special Ed applications the program area will be administering their own applications internally.
	N/A	YES	IEP PTP Role Admin	Assigns user roles to the IEP PTP application for DPI users.	CST	Jeff Perry & Derew Osborne	
	N/A	YES	Spec Ed Discretionary Grants Role Admin	Assigns user roles to the Special Ed Discretionary Grants application for DPI users.	CST	Jeff Perry & Derew Osborne	
ASM Access Viewer and Secure Admin Lookup	YES	YES	AV_AllApps	Staff at DPI who help to support our users including CST, DWDS, OEA, Special Ed, and others.	IT All	Jeff Perry & Derew Osborne	

College and Career Ready (CCR-IEP) - Manager	YES	YES	Administrator	Role can create/modify/delete questions and pathways in the CCR-IEP Application. Usually would just be SPED Developers, Data Coordinator, and DPI Consultants as needed.	Special Ed	LeAnn Leahy & Mike Fuller	Management portal for CCR-IEP Application
Combined Reporting	YES	YES	DPI Reader	Same privileges as DPI SFS Administrator but read-only access. – Not yet implemented	SFS	Scott Huelsman & Dan Bush	
			DPI SFS Administrator	Full access to the entire application MINUS system administration screens.			
			DPI Super Administrator	Full access to the entire application, including system administration screens.			
CTE Technical Incentive Grant (TIG)	YES	YES	Support	DPI Support role by CTE team	Core Apps	Josh Roy	
			DPI Admin	DPI role for Core Apps to configure yearly system settings and test issues.			
			DPI View	DPI Support read only role for CTE team and other DPI			
CTEskills DPI Admin	YES	YES	Admin	DPI CTE and Core Apps role to manage system wide configurations and all system data for troubleshooting.	Core Apps	Josh Roy	
DPI Application Security Manager (ASM)	YES	YES	DPIASMRoleAdmin	DPI Admin who can assign DPI staff to a role and setup a District Administrator.	IT All	Jeff Perry	
DPI Staff Directory	YES	YES	Read	Ability to connect to the database level and pull queries. No updates.	Core Apps	Josh Roy	
			Write	ASM Access to the application. Allows records to be added and updated via WAMS login.			

ECCP (Early College Credit Program)	YES	YES	Admin	ASM Access to the application. Allows all admin functions.	Core Apps	Josh Roy	
ECIDS Application	NO	NO (Domain Accounts created by DET)	App Admins	ECIDS Administrators Unrestricted access to all the features\functions in the ECIDS web portal.	DWDS	Melissa Straw	
			App Users	ECIDS Users General role for all the users with restricted access to the ECIDS web portal.			
			Webservice Users	ECIDS Webservice Users - Only Service Accounts will be in this group. - Service account credentials are used to submit data through web service.			
Ed-Fi Credential	YES	YES	AllFunctions	DPI admin view that provides the ability to manage vendors, vendor users, claimsets, profiles and education organization assignment to a WISEdata Ed-Fi 'application'. Most appropriate for DPI Collections and CST Manager and or CST Leads.	Collections	John Raub	
			AdminRead	DPI admin view that provides the ability to view vendors, vendor users, claimsets, profiles and education organization assignment to a WISEdata Ed-Fi 'application', but no changes can be made. Most appropriate for DPI or CESA help desk who need to answer questions but aren't authorized to make changes.			

EPP Program Information Manager	YES	YES	AllFunctions	CanDoAllFunctions	TeachSmart	Philip Crawford	
GED	YES	YES	AddUpdateTestCenters	Allows DPI Staff to Update Test Centers in the GED application.	Core Apps	Josh Roy	
			PrintTranscripts	Allows DPI Staff to Print GED Certificates from the GED application.			
			AddUpdateNewStudents	Allows DPI Staff to Update Students in the GED application.			
			UploadData	Allows DPI Staff to Upload information in the GED application.			
PTP - Post-Secondary Transition Plan	YES	YES	IEP_DPI_Admin	Role can access Admin level reports and all District entries. Cannot create/modify/save changes to district data.	Special Ed	LeAnn Leahy & Mike Fuller	
SAFA	YES		MSAccountant	Sets-up budgets & activity codes in STAR to populate in SAFA	Enterprise	Jesila Jinnah	
			ProgramApprover	Adds Grants, Programs & Projects, Approves budgets & allocations			
			AIDAccountant	Sets-up Allocations and makes voucher payments			
			Admin	Reconciles AD Accountants Vouchers for Payments, Process/submit weekly payments to STAR			
School Directory	YES	YES	DirectoryUpdate	DPI staff, specifically Apps Dev or DWDS, would use for updating Sch Dir info for an individual district or school.	CST	Lorraine Gardner	
School Directory DPI Admin	YES	YES	DPIDirectoryAdmin	This role is only for DPI staff on CST who would use when they need access to	CST	Lorraine Gardner	

				update every district or school and want to pick the district or school from a list.			
Secure Access File Exchange	Yes	YES	AllReports	Teams at DPI such as OEA and OSA who work with our users on these reports.	DWDS	Melissa Straw	
			AccountabilityReportCards	Teams at DPI such as OEA and OSA who work with our users on these reports.			
			ACTNCRCWorkKeys	Teams at DPI such as OEA and OSA who work with our users on these reports.			
Secure Access File Exchange - Staff	YES	YES	IDTeacherData	Teams at DPI such as Policy and Budget who work with our users on these reports.	DWDS	Melissa Straw	
Special Education Discretionary Grants	YES	YES	Grant Director	Basic user, most SPED team employees would get this role.	Special Ed	LeAnn Leahy & Mike Fuller	DPI Internal App for creating and releasing Grant Applications.
			Director	Director of Special Education would get this role.			
			Assistant SPED Director	Assistant Special Education Director would get this role.			
			Administrator	This role is typically reserved for SPED Development Team, DPI Data Coordinator, and the Grant Specialist.			
Special Education Portal	YES	YES	Administrator	Users are granted Admin level access to all apps in the portal and portal administration controls. Some SPED team employees may request this role as it grants them access to Admin level reports.	Special Ed	LeAnn Leahy & Mike Fuller	Portal to various SPED Apps.

			DPI Consultant	Most SPED Team employees would get this role. It allows them to access apps with special filters for Consultants.			
			Accountant	This role has some limited abilities for Financial Services and WISEgrants users.			
SFS Team Tools	YES	YES	TeamMember	A non-developer who has access to all business-related aspects of the application (but no “superuser” access	Finance	Dan Bush	
			Developer	A “superuser” role that allows access and control to all aspects of the application.			
			Manager	Same as TeamMember but also allowed to approve certain forms			
Special Ed Portal - Preschool Transition	YES	YES	DPI Admin	Role has view rights specific to Birth to 3 Program notifications and referrals as well as edit rights to Indicator 12 reporting.	Special Ed	Nancy Fuhrman, Joe Plautz	
			DPI User	Role has view rights specific to Birth to 3 Program notifications and referrals as well as Indicator 12 reporting.			
Special Ed Portal - Pupil Non Discrimination	YES	YES	DistrictAdmin		Special Ed	Mike Fuller	
			DPI Admin	Can Do DPI Admin Functions			
TCERT	YES	YES	G-App-TEPDL-Users	Limited view only access for TEPDL staff	TeachSmart	Philip Crawford	
			G-App-TEPDL-SpecialAccess	View only access including IIR & SSN data			
			G-TEPDLDev-U	Limited view only access for Apps Dev			
TEPDL Audit	YES	YES	AuditUIClient	CanInvokeWebServices	TeachSmart	Philip Crawford	
			AuditUIViewer	CanViewData			

			AuditUIEditor	CanViewData, CanEditData			
			AuditUIAdmin	CanConfigureLookups, CanViewData, CanEditData			
TEPDL Background Check	YES	YES	Administrator	Admin User	TeachSmart	Philip Crawford	
			TEPDLReadOnly	CanDoTEPDLReadOnly			
			Investigator	CanInvestigate			
TEPDL DOR	YES	YES	DORUIClient	CanInvokeWebServices	TeachSmart	Philip Crawford	
			DORUIEditor	CanEditData			
			DORUIAdmin	CanConfigureLookups			
			DORUIViewer	CanViewData			
TEPDL PDP	YES	YES	PDPAdministrator	CanEnquirePDPForEducator, CanQueryLookups, CanQueryVerifications, CanQueryVerifications	TeachSmart	Philip Crawford	
			PDPServiceProvider	CanEnquirePDPForEducator, CanQueryLookups, CanSubmitForm			
			PDPUIViewer	CanEnquirePDPForEducator, CanQueryVerifications			
			PDPUICallSVC	CanEnquirePDPForEducator, CanQueryLookups, CanQueryVerifications, CanQueryVerifications			
Tuition Waiver	YES	YES	Developer		SMS	Tricia Collins	
			Manager				
			Team Member				

WISEdash	YES	YES	DetailAnalyst	DPI staff who need to view detail data to complete related job tasks and/or who help to support our users.	DWDS	Melissa Straw	
			DetailFAFSAAccess	Similar role to the DetailAnalyst role except the user will also have access to the FAFSA dashboard and information.			
			DetailEconomicIndicator	DPI staff who need to view detail economic data to complete related job tasks and/or who help to support our users.			
			SummaryAnalyst	DPI staff who need to view summary data to complete related job tasks and/or who help to support our users.			
WISEdata Portal DPI Admin		YES	AllFunctions	Role for DPI Admins (Collections and a select number of CST users) that provides the same functionality as an LEA plus all administration functions (e.g job queue, rule management, view any LEA, etc.) Primarily Collections and CST manager and team leads	Collections	John Raub	
			DataWarehouse	Role for DPI DWDS so they can manage L2 rule accept, reject and null logic.			
			SupportLevel2	Rule created for DPI CST that allows for most the access of AllFunctions role without access to most of the Admin pages.			
			Support	Rules created for DPI CESA support which allows the same access as an LEA as well			

				as the ability to toggle to any LEA via the Change Agency screen			
WISEgrants DPI Access	YES	YES	Standard DPI User	DPI Standard user - view access to application, additional privileges as assigned by WIGAM	T1/SPED	Matt Baier & Rachel Zellmer	
			WIGAM	DPI Superuser - allows user to view/edit all WISEgrants content			
WISEid	YES	YES	WISEID_DPIAdmin	DPI role with access to do anything in WISEid including configuration	Core Apps	Josh Roy	
			WISEID_DPIDPICESASupport	CESA role with limited functionality to support LEAs			
			WISEID_DPISupport	DPI CST role with ability to do support functions and anything districts can do			
			WISEID_DPIReference	DPI read only role			
			WISEID_DPISuperUser	DPI role with access to do anything excluding system configuration			
WISEstaff for DPI	YES	YES	WISESTAFF_DPIReference	DPI read only role	Core Apps	Josh Roy	
			WISESTAFF_DPISuperUser	DPI role with access to do anything excluding system configuration			
			WISESTAFF_DPISupport	DPI CST role with ability to do support functions and anything districts can do			
			WISESTAFF_DPIAdmin	DPI role with access to do anything in WISEstaff including configuration			
			WISESTAFF_DPIDPICESASupport	CESA role with limited functionality to support LEAs			

WiSFIP	YES	YES	DPI Reader	Same privileges as DPI SFS Administrator but read-only access. – Not yet implemented	SFS	Scott Huelsman & Dan Bush	
			DPI SFS Administrator	Full access to the entire application MINUS system administration screens.			
			DPI Super Administrator	Full access to the entire application, including system administration screens.			

Power BI Service (Web) and DPI Roles

Team Responsible for Setup: DWDS

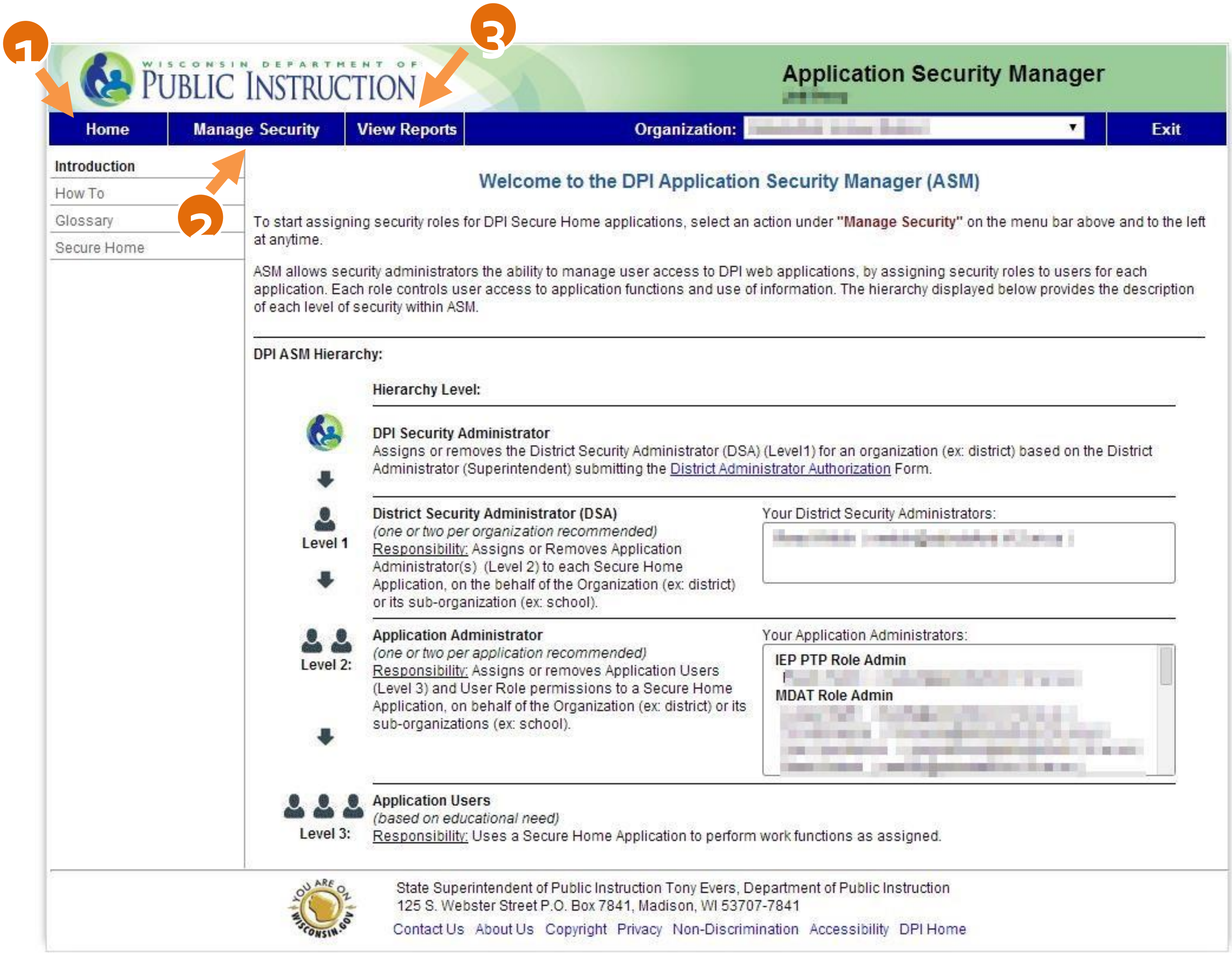
NOTE: WAMS ID not needed (internal AD account used for security)

Role	Role Desc	Team	Main Contact
O365SG-SPED-ServiceUsers	**1]** This Office 365 Security Group is created for the Special Ed Team. **2]** The users in this group are considered as 'Power Users' (a role in PBI) or Power BI 'Service Users'. **3]** The user(s) in this group will be able to **create reports/dashboards in Power BI Service only from the dataset published by Dataset Owners**. **4]** 'Service Users' should have access only to Power BI Service.	Special Ed	Vinod Dhanabalan
O365SG-SPED-DatasetOwners	**1]** This Office 365 Security Group is created for the Special Ed Team. **2]** The users in this group are considered as 'Super Users' (a role in PBI) or 'Dataset Owners' in Power BI Service. **3]** The user(s) in this group **own the published datasets and reports/dashboards** in Power BI Service. **4]** 'Dataset Owners' or 'Super Users' will have access to both Power BI Desktop and Power BI Service.	Special Ed	Vinod Dhanabalan

O365SG-SSPW-GeneralUsers	**1]** This Office 365 Security Group is created for the Student Services / Prevention and Wellness (SSPW) Team. **2]** The users in this group are considered as ‘Consumers’ (a role in PBI) or ‘General Users’ in Power BI Service. **3]** The user(s) in this group should be able to **only view** reports/dashboards in Power BI Service. **4]** ‘General Users’ should have access only to Power BI Service.	SSPW	Vinod Dhanabalan
O365SG-CoreApps-DatasetOwners	**1]** This Office 365 Security Group is created for the Core Apps Team. **2]** The users in this group are considered as ‘Super Users’ (a role in PBI) or ‘Dataset Owners’ in Power BI Service. **3]** The user(s) in this group **own the published datasets and reports/dashboards** in Power BI Service. **4]** ‘Dataset Owners’ or ‘Super Users’ will have access to both Power BI Desktop and Power BI Service.	Core Apps	Vinod Dhanabalan
O365SG-CoreApps-ServiceUsers	**1]** This Office 365 Security Group is created for the Core Apps Team. **2]** The users in this group are considered as ‘Power Users’ (a role in PBI) or Power BI ‘Service Users’. **3]** The user(s) in this group will be able to **create reports/dashboards in Power BI Service only from the dataset published by Dataset Owners**. **4]** ‘Service Users’ should have access only to Power BI Service.	Core Apps	Vinod Dhanabalan
O365SG-CST-GeneralUsers	**1]** This Office 365 Security Group is created for the Customer Services Team. **2]** The users in this group are considered as ‘Consumers’ (a role in PBI) or ‘General Users’ in Power BI Service. **3]** The user(s) in this group should be able to **only view** reports/dashboards in Power BI Service. **4]** ‘General Users’ should have access only to Power BI Service.	CST	Vinod Dhanabalan
O365SG-DPIDLITMgmtTeam	**1]** This Office 365 Security Group is created for the DPI DL IT Mgmt Team. **2]** The users in this group are considered as ‘Consumers’ (a role in PBI) or ‘General Users’ in Power BI Service. **3]** The user(s) in this group should be able to **only view** reports/dashboards in Power BI Service. **4]** ‘General Users’ should have access only to Power BI Service.	Dan Retzlaff & Melissa Straw	Vinod Dhanabalan
O365SG-DWDS-DatasetOwners	**1]** This Office 365 Security Group is created for the DWDS Team.	Melissa Straw	Vinod Dhanabalan

	2] The users in this group are considered as 'Super Users' (a role in PBI) or 'Dataset Owners' in Power BI Service. **3]** The user(s) in this group **own the published datasets and reports/dashboards** in Power BI Service. **4]** 'Dataset Owners' or 'Super Users' will have access to both Power BI Desktop and Power BI Service.		
O365SG-ITCHARGBCK-DatasetOwners	**1]** This Office 365 Security Group is created for Dan (Upon request, more users may be added in the future). **2]** The users in this group are considered as 'Super Users' (a role in PBI) or 'Dataset Owners' in Power BI Service. **3]** The user(s) in this group **own the published datasets and reports/dashboards** in Power BI Service. **4]** 'Dataset Owners' or 'Super Users' will have access to both Power BI Desktop and Power BI Service.	Dan Retzlaff & Melissa Straw	Vinod Dhanabalan
O365SG-OEA-DatasetOwners	**1]** This Office 365 Security Group is created for the OEA Team. **2]** The users in this group are considered as 'Super Users' (a role in PBI) or 'Dataset Owners' in Power BI Service. **3]** The user(s) in this group **own the published datasets and reports/dashboards** in Power BI Service. **4]** 'Dataset Owners' or 'Super Users' will have access to both Power BI Desktop and Power BI Service.	OEA	Vinod Dhanabalan
O365SG-PBIServiceAdmins	**1]** This Office 365 Security Group is created for the DWDS Team. **2]** The users in this group are considered as Power BI Service Administrators. **3]** Power BI Service Admins can **manage all the user permissions and security configurations available in the Power BI Service - Admin Portal**.	Melissa Straw	Vinod Dhanabalan

Application Security Manager (ASM) Quick Start Guide



Application Security Manager

[redacted]

Welcome to the DPI Application Security Manager (ASM)

To start assigning security roles for DPI Secure Home applications, select an action under **"Manage Security"** on the menu bar above and to the left at anytime.

ASM allows security administrators the ability to manage user access to DPI web applications, by assigning security roles to users for each application. Each role controls user access to application functions and use of information. The hierarchy displayed below provides the description of each level of security within ASM.

DPI ASM Hierarchy:

Hierarchy Level:

DPI Security Administrator
Assigns or removes the District Security Administrator (DSA) (Level1) for an organization (ex: district) based on the District Administrator (Superintendent) submitting the District Administrator Authorization Form.

Level 1
District Security Administrator (DSA)
(one or two per organization recommended)
Responsibility: Assigns or Removes Application Administrator(s) (Level 2) to each Secure Home Application, on the behalf of the Organization (ex: district) or its sub-organization (ex: school).

Your District Security Administrators:
[redacted]

Level 2:
Application Administrator
(one or two per application recommended)
Responsibility: Assigns or removes Application Users (Level 3) and User Role permissions to a Secure Home Application, on behalf of the Organization (ex: district) or its sub-organizations (ex: school).

Your Application Administrators:
IEP PTP Role Admin
[redacted]
MDAT Role Admin
[redacted]

Level 3:
Application Users
(based on educational need)
Responsibility: Uses a Secure Home Application to perform work functions as assigned.

State Superintendent of Public Instruction Tony Evers, Department of Public Instruction
125 S. Webster Street P.O. Box 7841, Madison, WI 53707-7841
Contact Us About Us Copyright Privacy Non-Discrimination Accessibility DPI Home

TOPIC TABS. Use these **menus to navigate ASM** to perform different tasks – you can view instructions and information to help you use the tool, manage or view the roles assigned to your district personnel or view reports.

1. **HOME.** Click on this tab to view the following:
   - The **Introduction** link is the Welcome page, explaining the ASM Hierarchy and displaying your district's District Security Administrators and Application Administrators for each application.
   - The **How To** page has complete instructions for performing all ASM-related tasks, including obtaining a WAMS ID, assigning and removing roles (see below), viewing reports, contacting the DPI Help Desk and more.
   - A **Glossary** with definitions for frequently used terms.

- A S**ecure Home** information page for information about Secure Home, how to log in and a link to return to the Secure Home menu.

2. **MANAGE SECURITY.** DSA's can use this tab to view or remove Application Administrators or assign a new Application Administrator. Application Administrators can use this tab to browse or edit Application Users or assign a user to a new role.
3. **VIEW REPORTS.** Here you can download reports in .CSV spread sheet format. These reports can be used to audit application users and administrators. View what roles are assigned to district personnel, the date roles were assigned and by whom, among other information. One report sorts by application, another by user.

To assign a new Application Administrator

The instructions below apply if you are a District Security Administrator for a district.

1. Hover your mouse over "Manage Security" on the blue menu bar for a list of dropdown selections
2. Click on "Assign a new Application Administrator"
3. Click on "Search Users" and fill in a minimum of 4 characters total in any field(s) listed to find and choose a WAMS user you want to assign as an Application Administrator
4. If there is more than one WAMS user for the search criteria entered, click on the radio button next to the WAMS user from the list displayed
5. Click on the "Role" dropdown field and select the Application Administrator Role you want to assign to the user selected 6. Click on the "Next" button
7. Review the confirmation page that is displayed to verify the user and role to be added
8. If you do not want to send an email notification to the user you want to add, uncheck the check box next to the "Notify user by email"
9. If you are sending an email notification to the user and want to carbon copy one other person, type the email address of the other person in the "Optional CC:" field
10. Click on the "OK" button
11. The successful completion pop up is displayed and click on the "Close" button

To assign an application level role to a user

The instructions below apply if you are an Application Administrator for an application.

1. Hover your mouse over "Manage Security" on the blue menu bar for a list of dropdown selections
2. Click on "Browse/Edit Application Users"
3. The Application Users and applications for the organization you are an administrator for, are displayed
4. Click on the 'x' icon next to the application user and role you would like to remove
5. Review the confirmation page that is displayed to verify the user and role to be removed
6. If you do not want the user you are removing to receive an email notification, uncheck the check box next to the "Notify user by email"
7. If you are sending an email notification to the user and want to carbon copy one other person, type the email address of the other person in the "Optional CC:" field
8. Click on the "OK" button
9. The successful completion pop up is displayed and click on the "Close" button

DO YOU NEED ACCESS? WOULD YOU LIKE MORE INFORMATION?

The Secure Home Information Page provides detailed information about how users can gain authorization, the three levels of security, how to obtain a WAMS ID and more. https://dpi.wi.gov/wise/secure-home-info

For a list of District Security Administrators and Application Administrators: https://apps2.dpi.wi.gov/ldsutil/admin/lookup

To view Student Data Privacy Information: https://dpi.wi.gov/wise/data-privacy/resources

DPI Data Contacts Inventory

Definitions

1. **Program Area Policy Data Steward** - The program area/team in this column is the team that owns this data and is responsible for this data. The specific contact is a team member of the program area that owns the data. This person typically knows and understands the federal and state laws and policies governing the collection of this data and can help identify what data elements are needed, business logic for those data elements, and due dates for collecting the data. This person would typically submit an IT Request to ask for a new data element to be collected. Example: Susan Piazza submitted an IT Request for Foster Care to be collected at the student level per ESSA requirements. In addition, this person typically provides guidance with how the data should be displayed based on reporting requirements and appropriate uses of the data. They might also complete "content" Quality Assurance (QA) of the dashboards as well.

   Responsibilities include:

   a. Participate in DPI's Data Steward Committee
   b. Communicate program policies, data needs, reporting requirements, and appropriate uses of the data.
   c. Know who else needs to be included in conversations around specific discussion items and decision items.
   d. Complete the data inventory.
   e. Determine definitions, collection frequency, and business rules for new data elements needed to meet reporting requirements.
   f. Discuss critical data issues within program area
   g. Assist the DPI Customer Services Team (CST) in generating communications and outreach to districts about data quality prior to snapshot, if appropriate.
   h. Help conduct internal audits of DPI data system users to ensure access is up to date. (Example: Melissa Straw sent out emails and reports to each Director listing team members who have access to WISEdash to confirm the access was still appropriate.
   i. Completing content QA of dashboards before production release to minimize data quality issues.
   j. Understand the basics of WISEdata and WISEdash to be able to answer general questions when asked.
   k. Understand where and how to direct LEAs who have specific technical support questions regarding WISEdata to CST.
   l. In cases where the CST may not have the deep understanding of complex questions around policy and business rules about the data being collected, the CST staff will connect with the program area data steward for assistance so they can help to have an accurate answer for the customer. CS staff will then respond back to the district.

2. **WISE Quality Assurance Data (QA) Steward -** This person reviews data for accuracy and points out discrepancies and errors. This person will work with the data at a detail level. This person should work very closely with the program area data steward to understand the rules behind the data. This person completes data testing for a particular topic by an agreed upon method between the data steward and IT. At a minimum, this would include viewing data through an application like WISEdash or reviewing a report.

   Responsibilities include:

   a. Participate in DPI's Data Steward committee
   b. Complete data quality review during WISEdata collections prior to snapshot which includes:
      i. Assisting in defining the most useful data reports used for reviewing data quality based on their knowledge of the data
      ii. Creating data reports for reviewing quality, if appropriate and if they possess technical skills needed
      iii. Reviewing data quality review reports
      iv. Collaboratively deliberating with IT staff, communications staff, and others as appropriate on best method for outreach follow up
      v. Conducting follow up and district outreach if the cross-team discussions suggest that is the best approach.
   c. Complete data and dashboard QA before implementation.
   d. Be aware of and understand the Common Education Data Standards (CEDS) and participate in reviews of new versions.
   e. Be aware of and use the DPI data governance processes, and follow procedures as far as data access, data requests, data QA, records management, data redaction, etc.
   f. Understand the basics of WISEdata and WISEdash to be able to answer general questions when asked.
   g. Understanding where and how to direct LEAs who have specific technical support questions around WISEdata to CST. This includes the understanding on how to create a help desk ticket.

h. In cases where the Customer Service Team may not have the deep understanding of complex questions around policy and business rules about the data being collected, the CS staff will connect with the quality assurance data steward for assistance so they can help to have an accurate answer for the customer.to determine the answer. CS staff will then respond back to the district.

3. **EDFacts Quality Assurance (QA) Data Steward -** This person will quality assure EDFacts files before they are submitted to the U.S. Department of Education by DPI's EDFacts Coordinator.. In this context, quality assurance includes checking state totals and subtotals for consistency (e.g. adding up the subtotal equals the total). It also includes checking year over year totals to ensure they are as expected. If the file also includes LEA data, totals for larger districts or district's with unique characteristics should also be reviewed, at the discretion of the Data Steward. In addition, when reviewing the files for a particular topic, if questions arise around totals for a specific demographic the QAer should work with the primary demographic data steward on any questions. This person may also work on the Consolidated School Performance Report (CSPR) with the EDFacts Coordinator.

WISEdata Customer Support

The Customer Services Team (CST) is the main point of contact for LEAs for any technical WISEdata related questions when an LEA is contacting us. Please direct LEAs to submit any questions regarding the WISEdata API, the WISEdata Data Quality Portal, error messages, or SIS Integration questions to the DPI Help Request Form. Their methods for supporting districts during the data collection process include: documentation, user group conference calls, training, WISEsupport through the CSN, completing support requests, vendor communications regarding specific customer issues, support State reporting discussions at vendor conferences, WISEdata conference, other DPI conferences, etc.

Note on Data Contacts

In most cases these contacts are our first stop when a discussion item or decision items comes up regarding a data topic, however, it does not mean that the contacts are the only contacts we connect with regarding work in a data topic area. For example, while OEA may be the program area owner of Grad Rate, there are many other teams that should weigh in on major decisions items and/or data collection and dashboard design. Most recently, we created a Grad Rate Workgroup consisting of team members from OEA, Title I, Special Education, Alternative Education, SSPW, SMS, and IT to discuss Grad Rate and Dropout Rate topics.

Another example would be the WISEdata Roster collection and reporting. To begin discussions on the topic the following groups were included: WISExplore, Policy and Budget, IT, Literacy and Mathematics, TEPDL, Staff Development, Arts Education, CTE, and OEA. This is because the roster collection includes coursework data, the student-teacher-link data, and is data that will be used by OEA and Policy and Budget for College and Career Readiness reporting, CCREWS, and more. WISExplore is included in most of our conversations as well since they work with the districts on WISEdata support and with using WISEdash for improvement planning.

Data Contacts

Data Group	Data Topic Area	1.Program Area Policy Data Steward	2.WISE QA Data Steward	3.EdFacts QA Data Steward
Library Data				N/A
LEA/School Data	LEA and School Data (data in the Enterprise data warehouse)	Team: CST, Apps Dev, DWDS, School Management Services Contact: CST Manager / Dan Retzlaff / Melissa Straw / Tricia Collins	Kari Tenley / Sheryl Cordell (choice)	Kari Tenley
	Charter School Authorizer Directory (data)	Team: School Management Services Contact: Cassi Benedict	Cassi Benedict	Kari Tenley / Cassi Benedict
	Charter Schools and Management Organizations	Team: School Management Services Contact: Cassi Benedict	Cassi Benedict	Cassi Benedict
	Virtual Schools	Team: School Management Services Contact: Cassi Benedict	Cassi Benedict	Kari Tenley / Cassi Benedict
	Graduation Requirements	Team: Teaching and Learning Contact: Tamara Mouw	Christine Tiedje	N/A
Basic Student Data	WISEid	Team: Apps Dev Contact: Josh Roy	Josh Roy	N/A
	TFS Enrollment / General Enrollment	Team: DWDS Contact: Melissa Straw	Melissa Aro / Rob Franke	Michelle Jones
	Open Enrollment (OPAL)	Team: School Management Services & OEA (for data warehouse loads) Contact: Tricia Collins & Laura Pinsonneault	Jen Danfield / Emily Colo (for data warehouse loads)	N/A

	Attendance / Chronic Absenteeism	Team: OEA Contact: Amy Marsman	Derek Field/Rob Franke (backup)	Rob Franke
	Discipline (related to Gun Free Schools Act or GFSA)	Team: SSPW TBD	TBD and/or Brian Dean	TBD
	Student Roster (coursework)	Team: Teaching and Learning, Literacy and Mathematics, Career and Technical Education Contact: Mai Choua Thao	Derek Field / Rob Franke (backup)	N/A
	Choice Student Data (WISEdata)	Team: OEA & School Management Services Contact: Laura Pinsonneault & Tricia Collins	Emily Colo	N/A
	Choice Student Data (OAS)	Team: School Management Services Contact: Tricia Collins	Sheryl Cordell	N/A
Student Demographic Data including Enrollment data grouped by these demographics	ELL Status/ELP Code	Team: Teaching and Learning and OSA Contact: Audrey Lesondak, Jesse Roberts	Audrey Lesondak / Jesse Roberts	N/A
	Migrant Status	Team: Title I Contact: Susan Piazza	Susan Piazza / Tena Torgerson	N/A
	Gender	Team: SSPW Contact: TBD	N/A	N/A
	Disability Status	Team: Special Education Contact: LeAnn Leahy	LeAnn Leahy	N/A
	Race/Ethnicity	Team: Special Education and Title I Contact: Courtney Reed Jenkins, Susan Piazza	N/A	N/A
	Homeless Status	Team: Title I Contact: Susan Piazza	Kristine Nadolski / Karen Rice	N/A

	Economic Status & Meal Service Eligibility	TBD	TBD	Michelle Jones
	Out of Home Care	Team: Title I Contact: Susan Piazza	Susan Piazza / Kyle Peaden	N/A
	Military Status	Team: SSPW Contact: TBD	Gregg Curtis	N/A
Special Education Data	Special Education Data	Team: Special Education Contact Courtney Reed Jenkins	LeAnn Leahy	N/A
	Special Education Data-Early Childhood	Team: Special Education Contact: Courtney Reed Jenkins	Nancy Fuhrman	N/A
	IDEA Child Count	Team: Special Education Contact: Courtney Reed Jenkins	LeAnn Leahy	LeAnn Leahy / Nancy Fuhrman
	IDEA Discipline	Team: Special Education Contact: Courtney Reed Jenkins	LeAnn Leahy	LeAnn Leahy
	IDEA Exiting	Team: Special Education Contact: Courtney Reed Jenkins	LeAnn Leahy	LeAnn Leahy
	IDEA Completion	Team: Special Education Contact: Courtney Reed Jenkins	LeAnn Leahy	LeAnn Leahy
	IDEA Personnel	Team: Special Education & TEPDL Contact: Courtney Reed Jenkins	LeAnn Leahy / Josh Kundert	LeAnn Leahy
	Coordinated Early Intervening Services (CEIS) (program)	Team: Special Education Contact: Courtney Reed Jenkins	Rachel Zellmer	LeAnn Leahy
	Maintenance of Effort (MOE) (program)	Team: Special Education Contact: Courtney Reed Jenkins	Rachel Zellmer	N/A

Other Specific Federal Reporting Data	Other Title I data (federal reporting)	Team: Title I Contact: Shelly Babler	Jessica Bartelt	Jessica Bartelt
	Neglected and Delinquent - Title I Part D	Team: Title I Contact: Susan Piazza	Kyle Peaden / Kristine Nadolski	Jessica Bartelt
	General Education Provisions Act (GEPA) - Federal Program Funding Allocations	Team: School Management Services Contact: Timothy Coulthart	Glenn Aumann	Glenn Aumann
Staff Data	Staff data collected through WISEstaff	TBD	TBD	TBD
	Staff data collected through WISEdata	TBD	TBD	TBD
	Staff data collected through WISEid	TBD	TBD	TBD
	Assignment Codes (annual list)	Team: TEPDL Contact: Julie Hagen	Josh Kundert	N/A
	Staff FTE	TBD	TBD	TBD
	Licensing	Team: TEPDL Contact: Julie Hagen	Josh Kundert	Julie Hagen / Josh Kundert
	Audit	Team: TEPDL Contact: Julie Hagen	Josh Kundert	Julie Hagen / Josh Kundert
	Inequitable Teacher Data	Team: DAE Contact: Sheila Briggs	Josh Kundert	Josh Kundert / Carl Frederick

Career and Technical Education	Consolidated Annual Report (CAR)	Team: CTE Contact: Sharon Wendt	Mai Choua Thao	Mai Choua Thao
	CTE Roster Data	Team: CTE Contact: Sharon Wendt	Mai Choua Thao	Mai Choua Thao
School Nutrition	School Nutrition Data	Team: Food and Nutrition Contact: Jessica Sharkus	Jessica Sharkus	N/A
Early Childhood	Early Childhood Data	Team: Content and Learning Contact: Sherry Kimball	Sherry Kimball	N/A
TI Data	Migrant Education Program	Team: Title I Contact: Susan Piazza	Susan Piazza / Tena Torgerson	Tena Torgerson / Cody Oltmans
	Homeless	Team: Title I Contact: Susan Piazza	Kristine Nadolski / Karen Rice	Jessica Bartelt
ELL Data (federal reporting)	Immigrant under Title III	Team: Teaching and Learning Contact: Audrey Lesondak	Audrey Lesondak	Audrey Lesondak
	Title III Teachers	Team: Teaching and Learning Contact: Audrey Lesondak	Audrey Lesondak	Jessica Bartelt / Audrey Lesondak
	Title III Students and Former Title III Students	Team: Teaching and Learning Contact: Audrey Lesondak	Audrey Lesondak	Michelle Jones / Emily Colo / Rob Franke
	LEP Enrolled	Team: Teaching and Learning Contact: Audrey Lesondak	Audrey Lesondak	Audrey Lesondak / Jesse Roberts
Assessment Data	ACCESS (English Language Proficiency Results)	Team: OSA & Teaching and Learning Contact: Jesse Roberts / Audrey Lesondak	Jesse Roberts / Derek Field / Emily Colo (backup)	Jesse Roberts

	ACT WorkKeys	Team: OSA Contact: Jennifer Bell	Duane Dorn / Phil Cranley / Rob Franke / Emily Colo (backup)	N/A
	ACT Aspire	Team: OSA Contact: Jennifer Bell	Phil Cranley / Duane Dorn (choice) / Emily Colo / Derek Field (backup)	N/A
	ACT Statewide	Team: OSA Contact: Jennifer Bell	Phil Cranley / Duane Dorn(choice) / Rob Franke / Emily Colo (backup)	Rob Franke / Kate Suchor
	Forward	Team: OSA Contact: Alison O'Hara	Phil Cranley / Duane Dorn(choice) / Derek Field / Kate Suchor (backup)	Rob Franke
	DLM / 1% SEA Cap	Team: OSA, Special Ed Contact: Michael Peacy / Phil Cranley / Daniel Parker	Phil Cranley / Emily Colo / Daniel Parker	Rob Franke
	ACT Graduates	TBD	Rob Franke	
	AP Exam	TBD	TBD	
Local Assessment Data	PALS	Team: OSA, Literacy and Mathematics, DWDS Contact: Duane Dorn / John Johnson / Melissa Straw	DPI contacts are a resource for data sharing discussions and the technical details around the data load. Testing happens to ensure the data loads correctly but we do not perform QA like we do for our statewide assessments since this is local data. Data is not used in public or federal reporting.	
	MAP	Team: OSA, DWDS Contact: Phil Olsen / Melissa Straw		
	Star	Team: OSA, DWDS Contact: Phil Olsen / Melissa Straw		

Accountability & Report Cards	Federal Accountability	Team: OEA Contact: Derek Field	Derek Field	Rob Franke
	State Report Cards - General	Team: OEA Contact: Emily Colo	Emily Colo	N/A
Student Outcome Data	Adjusted Cohort Graduation Rate	Team: OEA Contact: Laura Pinsonneault / Sam Bohrod	Rob Franke	Rob Franke
	High School Completion	Team: OEA, CTE Contact: Laura Pinsonneault / Nancy Molfenter	Nancy Molfenter / Rob Franke / Kate Suchor (backup)	Rob Franke
	Dropout Rate	Team: OEA, SSPW Contact: Sam Bohrod / Emily Colo / Gregg Curtis	Emily Colo / Rob Franke (backup) / Kate McCoy	Rob Franke
	Postsecondary Data	Team: OSA, OEA Contact: Jayson Chung / Sam Bohrod	Rob Franke / Derek Field (backup) / Jayson Chung (dashboard)	Rob Franke
Advanced Analytics Data	DEWS	Team: Policy and Budget Contact: Carl Frederick	Carl Frederick	N/A
	CCREWS	Team: Policy and Budget Contact: Justin Meyer	Justin Meyer	N/A
	Student Growth Percentiles (SGPs)	Team: OEA Contact: Derek Field	Derek Field / Kate Suchor (backup)	Rob Franke / Kate Suchor
	Value Added	Team: OEA Contact: Emily Colo	Emily Colo	N/A
	Achievement Gap	Team: Policy and Budget, OEA Contact: Carl Frederick / Justin Meyer / Laura Pinsonneault	Derek Field	N/A

Survey Data	School Climate	Team: SSPW Contact: TBD	TBD	N/A
	YRBS	Team: SSPW Contact: TBD	Kate McCoy	N/A
CSPR I	EdFacts Coordinator	Team: DWDS Contact: Yvette Johanson	N/A	N/A
	CSPR Certifier	Team: OSS Contact: Mary Jo Christiansen	N/A	N/A
	Assessments	Team: OEA, OSA Contact: Laura Pinsonneault / Viji Somasundaram	N/A	Rob Franke, Alison O'Hara
	Title III	Team: Teaching and Learning Contact: Audrey Lesondak	N/A	Rob Franke
	Homeless Program	Team: Title I Contact: Susan Piazza	N/A	Cody Oltmans
	Teachers Program (Title II-A)	Team: Educator Development & Support and TEPDL Contact: Abdallah Bendada / David Deguire	N/A	Josh Kundert / Carl Frederick
CSPR II	EdFacts Coordinator	Team: DWDS Contact: Yvette Johanson	N/A	N/A
	CSPR Certifier	Team: OSS Contact: Mary Jo Christiansen	N/A	N/A
	Title I-A	Team: Title I Contact: Shelly Babler	N/A	Cody Oltmans

	Title I-C (Migrant)	Team: Title I Contact: Susan Piazza, Tena Torgerson	N/A	Cody Oltmans
	Title I-D (Neglected or Delinquent)	Team: Title I Contact: Susan Piazza	N/A	Cody Oltmans
	Accountability	Team: OEA Contact: Laura Pinsonneault	N/A	Rob Franke

Notes on use cases for Economic Status data:

- District and School Accountability Report Cards for state reporting purposes
- Title I Federal Accountability reporting - Assessment, Adjusted Cohort Graduation Rate and Poverty Quartiles for purposes of determining the number of inexperienced, emergency/provisional credentialed, and out-of-field teachers in high and low poverty schools.
- CTE reporting for the Consolidated Annual Report.
- Title I Funding Allocations
- IDEA Funding Allocations
- WISEdash and EDFacts reporting (except C033 Free and Reduced Price Lunch file)
- Loan forgiveness for teachers at Title I schools
- High Poverty Aid
- E-RATE (although not for CEP schools)
- PI 37 Grants for National Teacher Certification for National Board for Professional Teaching Standards (NBPTS) and Wisconsin Master Educator Assessment Process (WMEAP) Grants
- Site eligibility determinations for Summer Food Service Program, Afterschool Snack Program, Child and Adult Care Food Program (CACFP) participation as At-Risk Afterschool programs, Family Day Care Home Providers eligibility to receive high meal reimbursement rates
- Policy and Budget
- Data is also used for disaggregation and control variable purposes when evaluating program effectiveness, conducting needs assessment and other related activities
- RLIS Objectives
    - Objective 1: Districts receiving RLIS grants will show an increase in the percentage of economically disadvantaged students scoring at or above proficiency on the English Language Arts assessment.
    - Objective 2: Districts receiving RLIS grants will show an increase in the percentage of economically disadvantaged students scoring at or above proficiency on the Mathematics assessment.
    - Outcome 1: An increased percentage of students in the high-poverty districts receiving RLIS grants will graduate from high school college and career ready.

Sharing Confidential Data with External Researchers

What is a confidential Data Request?

Requests are considered "confidential" when they include either student-level data or data that is aggregated but not redacted. *Every* request for student-level data should be treated as a confidential request whether or not the requested data include sensitive personally identifiable information (SPII).

Why share data with researchers?

Our Data Warehouse is a tremendously rich source of information about our schools, teachers, and students. By tracking student outcomes longitudinally, we can assess change over time, a critical condition for causal investigation and determining the impact of an implemented program or policy. Allowing research partners access to these data helps us extract maximum value from the data we collect, increasing our capacity to make evidence-based decisions on behalf of Wisconsin's students. There is also a public good, as well-disseminated research produces generalized knowledge available for everyone to benefit from.

How do we decide which requests to approve?

The diagram at the bottom of the page outlines the confidential data request approval process.

This process is designed to streamline tasks as much as possible while still allowing invested stakeholders from across DPI a say in how data are used.

What should I do if I get a request or want to share confidential data with a researcher outside DPI?

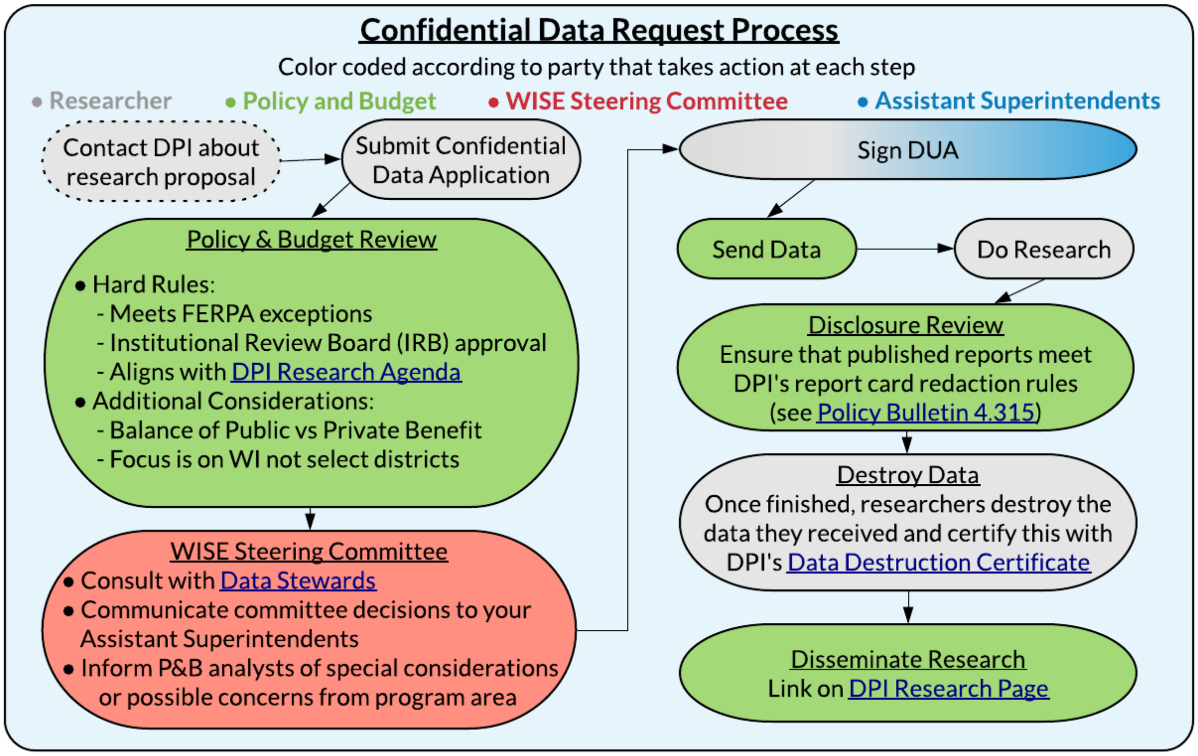
If you've received a request for student-level or unredacted data, please direct the requester to our Confidential Data Request webpage to begin the process.

Do open records requests use the same process?

No. If you receive an open records request, please direct it to Sam Morrison in the Office of the State Superintendent.

Further resources and contact information

Policy and Budget research analysts maintain DPI's current research agenda and a list of published research produced using DPI data in the research section of the Policy & Budget webpage.



Confidential Data Request Process

Color coded according to party that takes action at each step

● Researcher ● Policy and Budget ● WISE Steering Committee ● Assistant Superintendents

Contact DPI about research proposal

Submit Confidential Data Application

Policy & Budget Review

- Hard Rules:
  - Meets FERPA exceptions
  - Institutional Review Board (IRB) approval
  - Aligns with DPI Research Agenda
- Additional Considerations:
  - Balance of Public vs Private Benefit
  - Focus is on WI not select districts

WISE Steering Committee

- Consult with Data Stewards
- Communicate committee decisions to your Assistant Superintendents
- Inform P&B analysts of special considerations or possible concerns from program area

Sign DUA

Send Data

Do Research

Disclosure Review

Ensure that published reports meet DPI's report card redaction rules (see Policy Bulletin 4.315)

Destroy Data

Once finished, researchers destroy the data they received and certify this with DPI's Data Destruction Certificate

Disseminate Research

Link on DPI Research Page

Data Use Agreement

STATE OF WISCONSIN
DEPARTMENT OF PUBLIC INSTRUCTION

DATA USE AGREEMENT BETWEEN
Wisconsin Department of Public Instruction
and
Organization Name

This Data Use Agreement is made and entered into by and between the **Wisconsin Department of Public Instruction (DPI)**, hereafter "Holder," and **Organization Name**, hereafter "Recipient." Holder and Recipient agree to all of the following terms and conditions pursuant to which Holder will disclose certain confidential information in the form of a Data Set to Recipient:

1. Definitions

1.1. "Confidential Information" means any information that is not publicly available or is otherwise protected from disclosure by federal or state law, and includes personally identifiable information from an education record of a student, as those terms are defined in 34 C.F.R. § 99.3.

1.2. "Data Set" shall refer to data received as a result of queries incorporating the data warehouse elements specified in Appendix A.

1.3. "Project" means Recipient's study or project described under Section 2.

1.4. Terms used, but not otherwise defined, in this Agreement shall have the meaning given by the Family Educational Rights and Privacy Act's implementing regulations, 34 C.F.R. Part 99.

2. Project

2.1. Recipient seeks Confidential Information from Holder for the following reasons:

What is the purpose, scope and duration of this study/project?

2.2. The Project will have the following research benefits:

What is the research benefit? Include a description of the educational or other interests in the information.

3. Permitted Uses and Disclosures

3.1 Except as otherwise specified herein, Recipient may make all uses and disclosures of the Data Set necessary to conduct the Project.

4. Recipient Responsibilities

4.1 Recipient shall not use or disclose the Data Set for any purpose other than permitted by this Agreement pertaining to the Project, or as required by law. If disclosure of data other than that necessary to conduct the Project is deemed necessary, it shall take place only after prior notification of Holder.

4.2 Recipient shall use appropriate administrative, physical, and technical safeguards to prevent use or disclosure of the Data Set other than as provided for by this Agreement, including but not limited to the requirements in sections 7 through 10 below.

4.3 Recipient shall report to Holder any use or disclosure of the Data Set not provided for by this Agreement. The report shall be made within 24 hours of its discovery by Recipient, and Recipient shall comply with the requirements of section 5.2 below.

4.4 Recipient shall ensure that any agent, including a subcontractor, to whom it provides the Data Set, agrees to the same restrictions and conditions that apply through this Agreement to Recipient with respect to the Data Set.

4.5 Recipient shall not reidentify the information contained in the Data Set. Any reports or materials developed by Recipient or its subcontractors that use data provided under this Agreement shall not contain any personally identifiable information.

4.6 No later than ten (10) business days prior to release or publishing, Recipient shall submit to Holder for Holder's review all reports and materials developed under this agreement. The sole purpose for this review shall be to ensure that no personally identifiable information is included in the reports or materials. Holder shall use, as its basis for review, its internal redaction rules as they exist at the time the report is published or released. Holder shall make these redaction rules, currently contained in DPI Departmental Policy Bulletin 4.315, available to Recipient upon request.

4.7 Recipient may not contact the individuals who are the subject of Confidential Information contained in the Data Set.

5. Term, Breaches, and Termination

5.1 This Agreement shall be effective upon its execution by all signatories. This Agreement shall remain in effect until Termination Date mm/dd/yyyy or until all Confidential Information in the Data Set provided to Recipient is destroyed or returned to Holder, whichever comes first. Recipient will hold Confidential Information provided under this Agreement only as long as necessary to perform the work necessary for the Project. Recipient agrees to destroy all Confidential Information as soon as it is no longer needed for purposes of the Project.

5.2 Following a disclosure made in violation of this Agreement, Recipient shall do all of the following:

a. Notify Holder within 24 hours of discovering the violation.
b. Provide Holder, upon request, information regarding the violation and efforts to cure it.
c. Make every effort to cure the violation as soon as possible. If efforts to cure the violation are not successful within five business days of Recipient discovering the violation, Holder may, at its sole discretion, terminate this Agreement.

5.3 Holder may take any actions authorized by law to remediate the breach, including, without limitation, excluding Recipient from future access to data.

5.4 Both Holder and Recipient shall have the right to terminate this Agreement for any reason by providing sixty days' written notice to the other party.

6. General Provisions

6.1 Recipient and Holder understand and agree that individuals who are the subject of Confidential Information contained in the Data Set are not intended to be third party beneficiaries of this Agreement.

6.2 This Agreement shall not be assigned by Recipient without the prior express, written consent of Holder.

6.3 Each party agrees that it shall be responsible for its own acts and the results thereof to the extent authorized by law and shall not be responsible for the acts of the other party or the results thereof.

6.4 This is the full and complete agreement between the parties. This Agreement supersedes and replaces any prior agreement, whether verbal or in writing, concerning the subject matter of this Agreement. No amendment may be made to this Agreement unless it is in writing and signed by both parties.

7. Data Confidentiality and Security

7.1 Recipient shall implement and adhere to policies and procedures that restrict access to the Data Set. Recipient shall maintain, in writing, a complete list of individuals with access to the Data Set.

7.2 Persons retrieving data or using data from the Data Set may not copy or duplicate any confidential individual-level data for any reason. Examples of copying or duplicating include, but are not limited to, copying data to laptops, desktop computers, flash drives, compact discs, cloud storage, and flash/USB drives. Recipient may include data from the Data Set outside secured storage if all of the following apply:

a. The data is included in a project report's tables or charts.
b. The data is not personally identifiable and has been summarized and redacted based on rules determined by Holder.

7.3 Recipient shall require all individuals permitted by Recipient to use or receive the Data Set to read and agree to the terms of this Data Use Agreement. Recipient shall ensure such individuals have received training in personally identifiable information and the federal and state laws applicable to the use of personally identifiable information. General training materials on those topics are located at: http://dpi.wi.gov/wise/data-privacy/overview.

8. Transmission of Data

8.1 Holder shall send the Data Set and all confidential data to Recipient via a secure file transfer protocol (SFTP) or other method selected by Holder.

8.2 During this transmission, the Data Set shall be secured based upon a method selected by Holder.

9. Data Storage

9.1. The Data Set and all confidential data shall be kept, for a period not to exceed the estimated study length, in an encrypted electronic format by Recipient.

10. Data Destruction

10.1 Recipient shall destroy all Confidential Information connected with the Project when it is no longer needed for the purposes for the Project.

10.2 Recipient shall provide Holder electronic notice of planned destruction of records at least thirty (30) days prior to such destruction by completing the DPI's Electronic Data Destruction Form, which is located at: **http://dpi.wi.gov/wise/data-requests/certificate-data-destruction**

10.3 Recipient shall permanently erase all Confidential Information and Data Set from Recipient's storage devices upon completion or termination of the project. Recipient shall provide Holder with written notice of compliance with the data destruction provisions within five business days of destroying the data.

11. Data Elements

11.1 Attached is the data-specific appendix (Appendix A) listing the applicable educational element groupings to be provided by Holder to Recipient for use with the Project. All data remains the property of Holder.

IN WITNESS WHEREOF, the parties hereto execute this agreement as follows:

Wisconsin Department of Public Instruction
125 S. Webster Street
Madison, WI 53707-7841

Date: ___________________________ By: __________________________________
Keona S. Jones, Assistant State Superintendent
Division for Student and School Success

Date: ___________________________ By: __________________________________
Sheila Briggs, Assistant State Superintendent
Division for Academic Excellence

Date: ___________________________ By: __________________________________
Kurt J. Kiefer, Assistant State Superintendent
Division for Libraries and Technology

Date: ___________________________ By: __________________________________
Robert A. Soldner, Assistant State Superintendent
Division for Finance and Management

Date: ___________________________ By: __________________________________
Barbara Van Haren, Assistant State Superintendent
Division for Learning Support

Org. Name: ______________________________

Address: ________________________________

____

Date: ___________________________ By: ____________________________________

Name: ________________________________

Title: _________________________________

Appendix A

Data Topics Included in Request

□ ACT
□ ACCESS for ELLs
□ AP
□ WSAS (WKCE & WAA-SwD, Forward, Badger, Aspire, and/or ACT 11)
□ Attendance
□ Enrollment
□ Retention
□ Mobility
□ High school completion/dropout
□ Postsecondary enrollment
□ Discipline
□ Course enrollment

□ **Public school finance data**
□ **Youth Risk Behavior Survey data - middle school**
□ **Youth Risk Behavior Survey data - high school**

□ Disability status indicators
□ Socio-economic status indicators
□ Demographics (gender, race/ethnicity, English language learner status, migrant status)
□ Student identifiers (ID number, name, birthdate)

Extract Details:

In accordance with the identified target population, the data elements specified herein are to be extracted for the **** academic year(s).

Recipient will be contacted by DPI staff to coordinate data extraction **within 3 weeks of data use agreement finalization.**

118.125 Pupil records. (1) DEFINITIONS. In this section:

(a) "Behavioral records" means those pupil records that include psychological tests, personality evaluations, records of conversations, any written statement relating specifically to an individual pupil's behavior, tests relating specifically to achievement or measurement of ability, the pupil's physical health records other than his or her immunization records or any lead screening records required under s. 254.162, law enforcement officers' records obtained under s. 48.396 (1) or 938.396 (1) (b) 2. or (c) 3., and any other pupil records that are not progress records.

(b) "Directory data" means those pupil records which include the pupil's name, address, telephone listing, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, photographs, degrees and awards received and the name of the school most recently previously attended by the pupil.

(be) "Law enforcement agency" has the meaning given in s. 165.83 (1) (b).

(bL) "Law enforcement unit" means any individual, office, department, division, or other component of a school district that is authorized or designated by the school board to do any of the following:

1. Enforce any law or ordinance, or refer to the appropriate authorities a matter for enforcement of any law or ordinance, against any person other than the school district.

2. Maintain the physical security and safety of a public school.

(bs) "Law enforcement unit records" means records maintained by a law enforcement unit that were created by that law enforcement unit for the purpose of law enforcement.

(c) "Progress records" means those pupil records which include the pupil's grades, a statement of the courses the pupil has taken, the pupil's attendance record, the pupil's immunization records, any lead screening records required under s. 254.162 and records of the pupil's school extracurricular activities.

(cm) "Pupil physical health records" means those pupil records that include basic health information about a pupil, including the pupil's immunization records, an emergency medical card, a log of first aid and medicine administered to the pupil, an athletic permit card, a record concerning the pupil's ability to participate in an education program, any lead screening records required under s. 254.162, the results of any routine screening test, such as for hearing, vision or scoliosis, and any follow−up to such test, and any other basic health information, as determined by the state superintendent.

(d) "Pupil records" means all records relating to individual pupils maintained by a school but does not include any of the following:

1. Notes or records maintained for personal use by a teacher or other person who is required by the state superintendent under s. 115.28 (7) to hold a certificate, license, or permit if such records and notes are not available to others.

2. Records necessary for, and available only to persons involved in, the psychological treatment of a pupil.

3. Law enforcement unit records.

(e) "Record" means any material on which written, drawn, printed, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics.

(2) CONFIDENTIALITY AND DISCLOSURE OF PUPIL RECORDS. All pupil records maintained by a public school shall be confidential, except as provided in pars. (a) to (q) and sub. (2m). The school board shall adopt policies to maintain the confidentiality of such records and may adopt policies to promote the disclosure of pupil records and information permitted by law for purposes of school safety.

(a) A pupil, or the parent or guardian of a minor pupil, shall upon request, be shown and provided with a copy of the pupil's progress records.

(b) An adult pupil or the parent or guardian of a minor pupil shall, upon request, be shown, in the presence of a person qualified to explain and interpret the records, the pupil's behavioral records. Such pupil or parent or guardian shall, upon request, be provided with a copy of the behavioral records.

(c) 1. The judge of any court of this state or of the United States shall, upon request, be provided by the school district clerk or his or her designee with a copy of all progress records of a pupil who is the subject of any proceeding in such court.

2. Names of dropouts shall be provided to a court in response to an order under s. 118.163 (2m) (b).

(cg) The school district clerk or his or her designee shall provide a law enforcement agency with a copy of a pupil's attendance record if the law enforcement agency certifies in writing that the pupil is under investigation for truancy or for allegedly committing a criminal or delinquent act and that the law enforcement agency will not further disclose the pupil's attendance record except as permitted under s. 938.396 (1) (a). A school district clerk or designee who discloses a copy of a pupil's attendance record to a law enforcement agency for purposes of a truancy investigation shall notify the pupil's parent or guardian of that disclosure as soon as practicable after that disclosure.

(ch) The school district clerk or his or her designee shall provide a fire investigator under s. 165.55 (15) with a copy of a pupil's attendance record if the fire investigator certifies in writing that the pupil is under investigation under s. 165.55, that the pupil's attendance record is necessary for the fire investigator to pursue his or her investigation and that the fire investigator will use and further disclose the pupil's attendance record only for the purpose of pursuing that investigation.

(ck) The school district clerk or his or her designee shall make pupil records available for inspection or, upon request, disclose the contents of pupil records to authorized representatives of the department of corrections, the department of health services, the department of justice, or a district attorney for use in the prosecution of any proceeding or any evaluation conducted under ch. 980, if the pupil records involve or relate to an individual who is the subject of the proceeding or evaluation. The court in which the proceeding under ch. 980 is pending may issue any protective orders that it determines are appropriate concerning pupil records made available or disclosed under this paragraph. Any representative of the department of corrections, the department of health services, the department of justice, or a district attorney may disclose information obtained under this paragraph for any purpose consistent with any proceeding under ch. 980.

(cm) If school attendance is a condition of a child's dispositional order under s. 48.355 (2) (b) 7. or 938.355 (2) (b) 7., the school board shall notify the county department that is responsible for supervising the child within 5 days after any violation of the condition by the child.

(d) Pupil records shall be made available to persons employed by the school district which the pupil attends who are required by the department under s. 115.28 (7) to hold a license, law enforcement officers who are individually designated by the school board and assigned to the school district, and other school district officials who have been determined by the school board to have legitimate educational interests, including safety interests, in the pupil records. Law enforcement officers' records obtained under s. 938.396 (1) (c) 3. shall be made available as provided in s. 118.127. A school board member or an employee of a school district may not be held personally liable for any damages caused by the nondisclosure of any information specified in this paragraph unless the member or employee acted with actual malice in failing to disclose the information. A school district may not be held liable for any damages caused by the nondisclosure of any information specified in this paragraph unless the school district or its agent acted with gross negligence or with reckless, wanton, or intentional misconduct in failing to disclose the information.

(e) Upon the written permission of an adult pupil, or the parent or guardian of a minor pupil, the school shall make available to the person named in the permission the pupil's progress records or such portions of the pupil's behavioral records as determined by the person authorizing the release. Law enforcement officers' records obtained under s. 48.396 (1) or 938.396 (1) (b) 2. or (c) 3. may not be made available under this paragraph unless specifically identified by the adult pupil or by the parent or guardian of a minor pupil in the written permission.

(f) Pupil records shall be provided to a court in response to subpoena by parties to an action for in camera inspection, to be used only for purposes of impeachment of any witness who has testified in the action. The court may turn said records or parts thereof over to parties in the action or their attorneys if said records would be relevant and material to a witness's credibility or competency.

(g) 1. The school board may provide any public officer with any information required to be maintained under chs. 115 to 121.

2. Upon request by the department, the school board shall provide the department with any information contained in a pupil record that relates to an audit or evaluation of a federal or state− supported program or that is required to determine compliance with requirements under chs. 115 to 121.

(h) Information from a pupil's immunization records shall be made available to the department of health services to carry out the purposes of s. 252.04.

(hm) Information from any pupil lead screening records shall be made available to state and local health officials to carry out the purposes of ss. 254.11 to 254.178.

(i) Upon request, the school district clerk or his or her designee shall provide the names of pupils who have withdrawn from the public school prior to graduation under s. 118.15 (1) (c) to the technical college district board in which the public school is located or, for verification of eligibility for public assistance under ch. 49, to the department of health services, the department of children and families, or a county department under s. 46.215, 46.22, or 46.23.

(j) 1. Except as provided under subds. 2. and 3., directory data may be disclosed to any person, if the school has notified the parent, legal guardian or guardian ad litem of the categories of information which it has designated as directory data with respect to each pupil, has informed the parent, legal guardian or guardian ad litem of that pupil that he or she has 14 days to inform the school that all or any part of the directory data may not be released without the prior consent of the parent, legal guardian or guardian ad litem and has allowed 14 days for the parent, legal guardian or guardian ad litem of that pupil to inform the school that all or any part of the directory data may not be released without the prior consent of the parent, legal guardian or guardian ad litem.

2. If a school has notified the parent, legal guardian or guardian ad litem that a pupil's name and address has been designated as directory data, has informed the parent, legal guardian or guardian ad litem of the pupil that he or she has 14 days to inform the school that the pupil's name and address may not be released without the prior consent of the parent, legal guardian or guardian ad litem, has allowed 14 days for the parent, legal guardian or guardian ad litem of the pupil to inform the school that the pupil's name and address may not be released without the prior consent of the parent, legal guardian or guardian ad litem and the parent, legal guardian or guardian ad litem has not so informed the school, the school district clerk or his or her designee, upon request, shall provide a technical college district board with the name and address of each such pupil who is expected to graduate from high school in the current school year.

3. If a school has notified the parent, legal guardian or guardian ad litem of the information that it has designated as directory data with respect to any pupil, has informed the parent, legal guardian or guardian ad litem of the pupil that he or she has 14 days to inform the school that such information may not be released without the prior consent of the parent, legal guardian or guardian ad litem, has allowed 14 days for the parent, legal guardian or guardian ad litem of the pupil to inform the school that such information may not be released without the prior consent of the parent, legal guardian or guardian ad litem and the parent, legal guardian or guardian ad litem has not so informed the school, the school district clerk or his or her designee, upon request, shall provide any representative of a law enforcement agency, district attorney, city attorney or corporation counsel, county department under s. 46.215, 46.22 or 46.23 or a court of record or municipal court with such information relating to any such pupil

enrolled in the school district for the purpose of enforcing that pupil's school attendance, investigating alleged criminal or delinquent activity by the pupil or responding to a health or safety emergency.

(k) A school board may disclose personally identifiable information from the pupil records of an adult pupil to the parents or guardian of the adult pupil, without the written consent of the adult pupil, if the adult pupil is a dependent of his or her parents or guardian under 26 USC 152, unless the adult pupil has informed the school, in writing, that the information may not be disclosed. (L) A school board shall disclose the pupil records of a pupil in compliance with a court order under s. 48.236 (4) (a), 48.345 (12) (b), 938.34 (7d) (b), 938.396 (1) (d), or 938.78 (2) (b) 2. after making a reasonable effort to notify the pupil's parent or legal guardian.

(m) A parent who has been denied periods of physical placement with a child under s. 767.41 (4) does not have the rights of a parent or guardian under pars. (a) to (j) with respect to that child's pupil records.

(n) For any purpose concerning the juvenile justice system and the system's ability to effectively serve a pupil, prior to adjudication:

1. A school board may disclose pupil records to a city attorney, corporation counsel, agency, as defined in s. 938.78 (1), intake worker under s. 48.067 or 938.067, court of record, municipal court, private school, or another school board if disclosure is pursuant to an interagency agreement and the person to whom the records are disclosed certifies in writing that the records will not be disclosed to any other person except as otherwise authorized by law. For the purpose of providing services to a pupil before adjudication, a school board may disclose pupil records to a tribal school if disclosure is pursuant to an agreement between the school board and the governing body of the tribal school and if the school board determines that enforceable protections are provided by a tribal school policy or tribal law that requires the tribal school official to whom the records are disclosed not to disclose the records to any other person except as permitted under this subsection.

2. A school board shall disclose pertinent pupil records to an investigating law enforcement agency or district attorney if the person to whom the records are disclosed certifies in writing that the records concern the juvenile justice system and the system's ability to effectively serve the pupil, relate to an ongoing investigation or pending delinquency petition, and will not be disclosed to any other person except as otherwise authorized by law.

(p) A school board may disclose pupil records to appropriate parties in connection with an emergency if knowledge of the information is necessary to protect the health or safety of any individual.

(q) On request, a school board may disclose pupil records that are pertinent to addressing a pupil's educational needs to a caseworker or other representative of the department of children and families, a county department under s. 46.215, 46.22, or 46.23, or a tribal organization, as defined in 25 USC 450b (L), that is legally responsible for the care and protection of the pupil, if the caseworker or other representative is authorized by that department, county department, or tribal organization to access the pupil's case plan. A department, county department, or tribal organization that receives pupil records under this paragraph may not further disclose those pupil records or any personally identifiable information contained in those pupil records except as follows:

1. To a person who is engaged in addressing the pupil's educational needs, who is authorized by that department, county department, or tribal organization to receive that disclosure, and to whom that disclosure is authorized under this section or under a substantially similar tribal law.

2. Upon request, to any court of this state or of the United States that needs to review those records or that information for the purpose of addressing the educational needs of a pupil who is the subject of a proceeding in that court.

3. In response to an order of a court conducting proceedings under s. 48.135, 48.21, 938.135, 938.18, 938.183, or 938.21, proceedings related to a petition under s. 48.13, 48.133, 48.42, 938.12, or 938.13, or dispositional proceedings under subch. VI or VIII of ch. 48 or subch. VI of ch. 938 or in response to a subpoena issued in such a proceeding, to any person who is engaged in addressing the educational needs of the pupil and who is authorized to receive that disclosure under that order or subpoena. Except as provided in 20 USC 1232g (b) (2) (B), a department,

county department, or tribal organization that is issued an order or subpoena described in this subdivision shall provide notice of the order or subpoena to the pupil's parent or guardian before complying with the order or subpoena.

(2m) CONFIDENTIALITY OF PUPIL PHYSICAL HEALTH RECORDS. (a) Except as provided in par. (b), any pupil record that relates to a pupil's physical health and that is not a pupil physical health record shall be treated as a patient health care record under ss. 146.81 to 146.84.

(b) Any pupil record that concerns the results of an HIV test, as defined in s. 252.01 (2m), shall be treated as provided under s. 252.15.

(3) MAINTENANCE OF RECORDS. Each school board shall adopt rules in writing specifying the content of pupil records and the time during which pupil records shall be maintained. No behavioral records may be maintained for more than one year after the pupil ceases to be enrolled in the school, unless the pupil specifies in writing that his or her behavioral records may be maintained for a longer period. A pupil's progress records shall be maintained for at least 5 years after the pupil ceases to be enrolled in the school. A school board may maintain the records on microfilm, on an optical disc, or in electronic format if authorized under s. 19.21 (4) (c), or in such other form as the school board deems appropriate. A school board shall maintain law enforcement officers' records obtained under s. 48.396 (1) or 938.396 (1) (b) 2. or (c) 3. separately from a pupil's other pupil records. Rules adopted under this subsection shall be published by the school board as a class 1 notice under ch. 985.

(4) TRANSFER OF RECORDS. No later than the next working day, a school district, a private school participating in the program under s. 118.60 or in the program under s. 119.23, and the governing body of a private school that, pursuant to s. 115.999 (3), 119.33(2) (c) 3., or 119.9002 (3) (c), is responsible for the operation and general management of a school transferred to an opportunity schools and partnership program under s. 119.33, subch. IX of ch. 115, or subch. II of ch. 119 shall transfer to another school, including a private or tribal school, or school district all pupil records relating to a specific pupil if the transferring school district or private school has received written notice from the pupil if he or she is an adult or his or her parent or guardian if the pupil is a minor that the pupil intends to enroll in the other school or school district or written notice from the other school or school district that the pupil has enrolled or from a court that the pupil has been placed in a juvenile correctional facility, as defined in s. 938.02 (10p), or a secured residential care center for children and youth, as defined in s. 938.02 (15g). In this subsection, "school" and "school district" include any juvenile correctional facility, secured residential care center for children and youth, adult correctional institution, mental health institute, or center for the developmentally disabled that provides an educational program for its residents instead of or in addition to that which is provided by public, private, and tribal schools.

(5) USE FOR SUSPENSION OR EXPULSION. (a) Except as provided in par. (b), nothing in this section prohibits a school district from using a pupil's records in connection with the suspension or expulsion of the pupil or the use of such records by a multidisciplinary team under ch. 115.

(b) Law enforcement officers' records obtained under s. 48.396 (1) or 938.396 (1) (b) 2. or (c) 3. and records of the court assigned to exercise jurisdiction under chs. 48 and 938 or of a municipal court obtained under s. 938.396 (2g) (m) may not be used by a school district as the sole basis for expelling or suspending a pupil or as the sole basis for taking any other disciplinary action against a pupil, but may be used as the sole basis for taking action against a pupil under the school district's athletic code.

(6) APPLICATION TO EXISTING RECORDS. Any records existing on June 9, 1974 need not be revised for the purpose of deleting information from pupil records to comply with this section.

(7) DISCLOSURE OF LAW ENFORCEMENT UNIT RECORDS. A school board shall treat law enforcement unit records of juveniles in the same manner as a law enforcement agency is required to treat law enforcement officers' records of juveniles under s. 938.396 (1) (a).

History: 1973 c. 254; 1977 c. 418; 1979 c. 205; 1981 c. 20, 273; 1983 a. 189; 1985 a. 218; 1987 a. 27, 70, 206, 285, 337, 355; 1987 a. 399 s. 491r; 1987 a. 403 ss. 123, 124, 256; 1989 a. 31, 168; 1989 a. 201 s. 36; 1989 a. 336; 1991 a. 39, 189; 1993 a. 27, 172, 334, 377, 385, 399, 450, 491; 1995 a. 27 ss. 3939, 3940, 9126 (19), 9130 (4), 9145 (1); 1995 a. 77, 173, 225, 352; 1997 a. 3, 27, 205, 237, 239; 1999 a. 9, 149; 2003 a. 82, 292; 2005 a. 344, 434; 2005 a. 443 s. 265; 2007 a. 20 ss. 2712, 9121 (6) (a); 2009 a. 11, 28, 209, 302, 309; 2011 a. 32, 105, 260; 2015 a. 55, 161, 196; 2017 a. 251.

A public school student's interim grades are pupil records specifically exempted from disclosure under s. 118.125. A failure to specifically state reasons for denying an open records request for records that are specifically exempted from disclosure does not compel disclosure of those records. State ex rel. Blum v. Board of Education, 209 Wis. 2d 377, 565 N.W.2d 140 (Ct. App. 1997), 96−0758.

A court need not wait until trial to disclose pupil records under sub. (2) (f) and may instead base its decision on the review of deposition testimony. Sub. (2) (f) refers to an action, which is a much broader term than trial. A witness who has been deposed has testified in the action. Anderson v. Northwood School District, 2011 WI App 31, 332 Wis. 2d 134, 796 N.W.2d 874, 09−1881.

A court may not disclose confidential records under sub. (2) (f) merely because they are relevant to a plaintiff's claim. The court's gatekeeper role is to protect the privacy of the pupil whose records are sought, releasing only those records that may concern a specific witness's credibility or competency. Anderson v. Northwood School District, 2011 WI App 31, 332 Wis. 2d 134, 796 N.W.2d 874, 09−1881.

When neither defense counsel nor the school was familiar with the requirements of sub. (2) (f) and neither wholly complied with the statute during discovery when the school faxed the records directly to defense counsel upon defense counsel's request for records rather than provide them to the court for *in camera* inspection, the trial court was not correct to prohibit the defense from using the records. The trial court should have, upon receipt of the documents, conducted the *in camera* inspection required by the statute, while requiring the parties to keep the documents confidential. State v. Echols, 2013 WI App 58, 348 Wis. 2d 81, 831 N.W.2d 768, 12−0422.

Pupil information that local education agencies are required to release to the department of public instruction under the reporting provisions of ch. 89, laws of 1973, may be provided, with or without permission, without violation of the state or federal confidentiality statutes. 65 Atty. Gen. 1.

"Pupil records" are "public records" under s. 19.32 (2) but are subject to special statutes that limit access and direct maximum and minimum periods of maintenance before destruction. 72 Atty. Gen. 169.

Access to student records in Wisconsin. 1976 WLR 975.

Wisconsin SLDS Pre-Site Visit:

PTAC Documentation Review

Overview:

The National Center for Educational Statistics (NCES) administers the Statewide Longitudinal Data Systems(SLDS) Grant Program and has engaged the Privacy Technical Assistance Center(PTAC) as a resource to aid in document review prior to SLDS grantee site visits.

PTAC, located within the Student Privacy Policy and Assistance Division, was established in 2010 as a "one-stop" resource for education stakeholders to learn about data privacy, confidentiality, and security practices related to student-level data systems and other uses of student data.

SLDS has engaged PTAC to conduct a pre-site visit review of data privacy and security documentation prior to regular site monitoring visits. This review is a culmination of the OIG Inspectors audit of the SLDS Program which identified the area of data privacy and security as an area of focus.

Approach:

PTAC provides regular services to educational entities such as providing official guidance on FERPA through the Student Privacy Help Desk, developing privacy and security training materials for states and districts, issuing privacy and security best practice recommendations including issue briefs and checklists, as well as conducting technical assistance site visits to SEAs and LEAs.

As a basis for this review, PTAC has primarily utilized the "Checklist: Data Governance" as well as the "Data Security Checklist", both developed to assist stakeholder organizations with establishing and maintaining a successful data governance and security program. The final resource used for this review was the "Written Agreement Checklist".

Documents Reviewed:

- 4.300 Student Data Access Policy
- 4.315 Confidentiality of Individual Pupil Data and Data Redaction (Policy)
- Acceptable Use Policy
- Confidentiality Training
- Data Access Request Limited Use
- Data Access Request through Footprints
- Data Governance at DPI (presentation)
- Data Governance Intranet Site Screen Shots
- Data Incident Template
- Data Quality Screenshots
- DPI CM Handbook
- DPI Data Contacts Inventory
- DPI Data Steward Committee
- DPI Data Use Agreement

Wisconsin SLDS Pre-Site Visit:

PTAC Documentation Review

- DPI Internal Data Access Request Process and Role Descriptions
- DUA UW Teach Ed Taskforce Studies
- DUA WEC ACP Eval
- IT Project Request
- Project Governance @ DPI
- Security and Privacy Review Guidelines-Documentation
- Snapshot Preparation - Detailed Guide
- Student Data Access Policy and Procedures Guidebook

Key Takeaways for Wisconsin:

The Wisconsin Department of Public Instruction (DPI) has done a thorough job identifying key areas within their organization that benefit from having a formal policy to address strategic aspects of data governance.

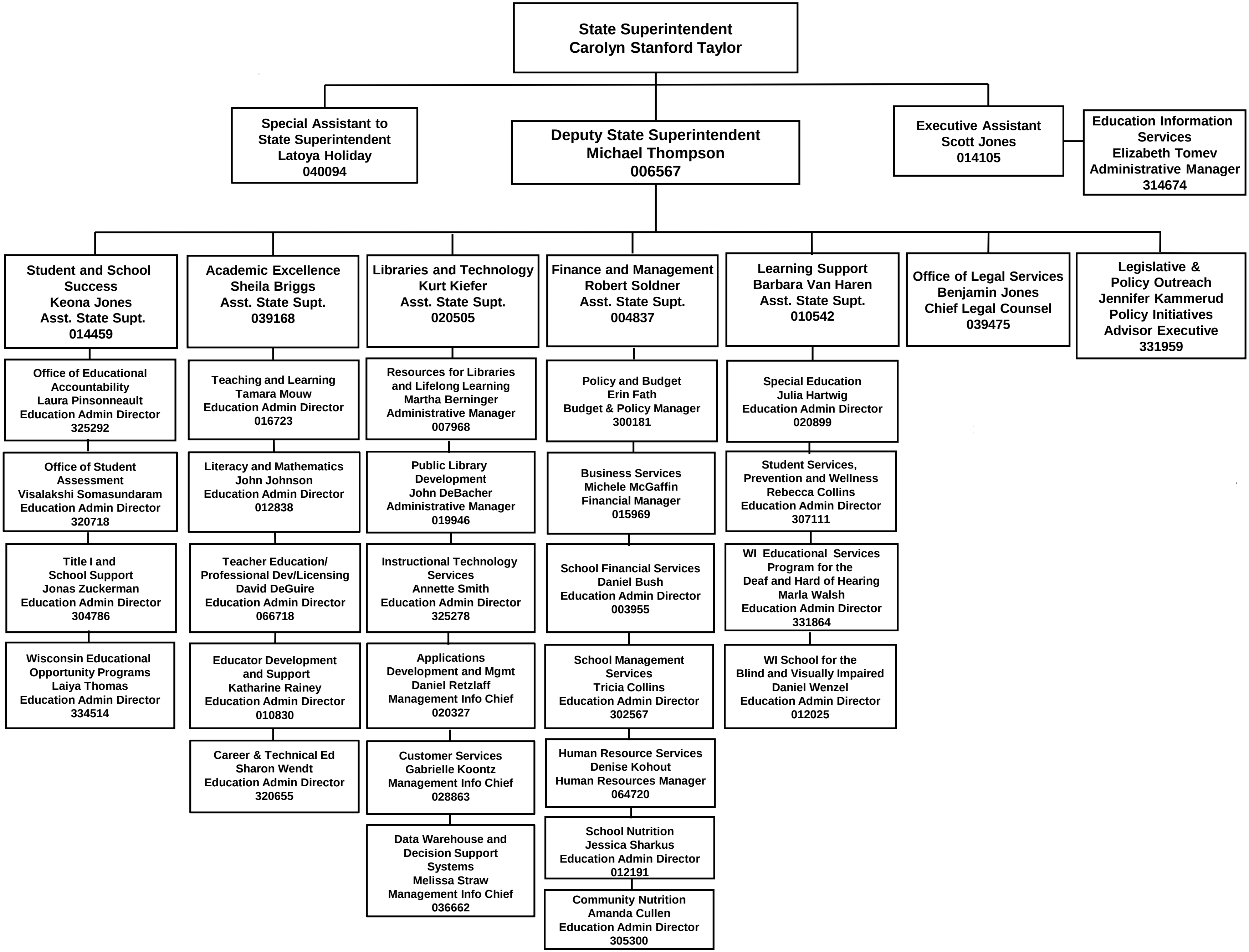
During the PTAC review, all areas critical to data governance were addressed through documentation provided by DPI. From organizational structure, governance roles and responsibilities, to processes for accessing and requesting data. PTAC was provided with a very complete picture of the data lifecycle in WI as it relates to the SLDS and education data management in the state. Written agreements provided for review, also met requirements and best practices.

Wisconsin has demonstrated one of the most robust and comprehensive data security and management programs that have been reviewed as part of the SLDS Site Visits since the SLDS program has begun to focus on data security and privacy. By ingraining governance throughout the enterprise, Wisconsin has continued to provide a high standard for student data privacy and security.

Key Takeaways for Program Officers and SST;

During review of the documentation provided by Wisconsin, all documentation met the standard of addressing areas PTAC considers best practices, if not establishing a bar for new best practices. PTAC also reviewed written agreements for data sharing.

From a documentation review, WI has demonstrated a well-organized and mature data governance program. Other states would do well to learn from Wisconsin, as an example of addressing data privacy through the implementation and administration of effective data governance.



State Superintendent
Carolyn Stanford Taylor

Special Assistant to
State Superintendent
Latoya Holiday
040094

Deputy State Superintendent
Michael Thompson
006567

Executive Assistant
Scott Jones
014105

Education Information
Services
Elizabeth Tomev
Administrative Manager
314674

Student and School
Success
Keona Jones
Asst. State Supt.
014459

Office of Educational
Accountability
Laura Pinsonneault
Education Admin Director
325292

Office of Student
Assessment
Visalakshi Somasundaram
Education Admin Director
320718

Title I and
School Support
Jonas Zuckerman
Education Admin Director
304786

Wisconsin Educational
Opportunity Programs
Laiya Thomas
Education Admin Director
334514

Academic Excellence
Sheila Briggs
Asst. State Supt.
039168

Teaching and Learning
Tamara Mouw
Education Admin Director
016723

Literacy and Mathematics
John Johnson
Education Admin Director
012838

Teacher Education/
Professional Dev/Licensing
David DeGuire
Education Admin Director
066718

Educator Development
and Support
Katharine Rainey
Education Admin Director
010830

Career & Technical Ed
Sharon Wendt
Education Admin Director
320655

Libraries and Technology
Kurt Kiefer
Asst. State Supt.
020505

Resources for Libraries
and Lifelong Learning
Martha Berninger
Administrative Manager
007968

Public Library
Development
John DeBacher
Administrative Manager
019946

Instructional Technology
Services
Annette Smith
Education Admin Director
325278

Applications
Development and Mgmt
Daniel Retzlaff
Management Info Chief
020327

Customer Services
Gabrielle Koontz
Management Info Chief
028863

Data Warehouse and
Decision Support
Systems
Melissa Straw
Management Info Chief
036662

Finance and Management
Robert Soldner
Asst. State Supt.
004837

Policy and Budget
Erin Fath
Budget & Policy Manager
300181

Business Services
Michele McGaffin
Financial Manager
015969

School Financial Services
Daniel Bush
Education Admin Director
003955

School Management
Services
Tricia Collins
Education Admin Director
302567

Human Resource Services
Denise Kohout
Human Resources Manager
064720

School Nutrition
Jessica Sharkus
Education Admin Director
012191

Community Nutrition
Amanda Cullen
Education Admin Director
305300

Learning Support
Barbara Van Haren
Asst. State Supt.
010542

Special Education
Julia Hartwig
Education Admin Director
020899

Student Services,
Prevention and Wellness
Rebecca Collins
Education Admin Director
307111

WI Educational Services
Program for the
Deaf and Hard of Hearing
Marla Walsh
Education Admin Director
331864

WI School for the
Blind and Visually Impaired
Daniel Wenzel
Education Admin Director
012025

Office of Legal Services
Benjamin Jones
Chief Legal Counsel
039475

Legislative &
Policy Outreach
Jennifer Kammerud
Policy Initiatives
Advisor Executive
331959

National Institute of Standards and Technology

Cybersecurity Framework and Assessment

Control Objective Number/Title	**Control Objective**
Obj 1 - ID.AM: Identify Asset Management	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization’s risk strategy.
Obj 2 - ID.BE: Identify Business Environment	**Business Environment (ID.BE):** The organization’s mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
Obj 3 - ID.GV: Identify Governance	**Governance (ID.GV):** The policies, procedures, and processes to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
Obj 4 - ID.RA: Identify Risk Assessment	**Risk Assessment (ID.RA):** The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
Obj 5 - ID.RM: Identify Risk Management Strategy	**Risk Management Strategy (ID.RM):** The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
Obj 6 - PR.AC: Protect Access Control	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions. ITGC: (1)Access controls over infrastructure, applications, and data (2) Computer Operation Controls

Obj 7 - PR.AT: Protect Awareness and Training	**Awareness and Training (PR.AT):** The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.
Obj 8 - PR.DS: Protect Data Security	**Data Security (PR.DS):** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
Obj 9 - PR.IP: Protect Information Protection Processes and Procedures	**Information Protection Processes and Procedures (PR.IP):** Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
Obj 10 - PR.MA: Protect Maintenance	**Maintenance (PR.MA):** Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.
Obj 11 - PR.PT: Protect Protective Technology	**Protective Technology (PR.PT):** Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.
Obj 12 - DE.AE Detect Anomalies and Events	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.
Obj 13 - DE.CM: Detect Security Continuous Monitoring	**Security Continuous Monitoring (DE.CM):** The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.
Obj 14 - DE.DP: Detect Detection Processes	**Detection Processes (DE.DP):** Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.
Obj 15 - RS.RP: Respond Response Planning	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.

Obj 16 - RS.CO: Respond Communications	**Communications (RS.CO):** Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.
Obj 17 - RS.AN: Respond Analysis	**Analysis (RS.AN):** Analysis is conducted to ensure adequate response and support recovery activities.
Obj 18 - RS.MI: Respond Mitigation	**Mitigation (RS.MI):** Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.
Obj 19 - RS.IM: Respond Improvements	**Improvements (RS.IM):** Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.
Obj 20 - RC.RP: Recover Recovery Plan	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.
Obj 21 - RC.IM: Recover Improvements	**Improvements (RC.IM):** Recovery planning and processes are improved by incorporating lessons learned into future activities.
Obj 22 - RC.CO Recover Communications	**Communications (RC.CO):** Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.