Student Data Access: Policy 4.300 & Confidentiality of Individual Pupil Data and Data Redaction: Policy 4.315

Procedures Guidebook

The Wisconsin Department of Public Instruction complies with federal and state laws to collect, store, maintain, and report student data. Because department management and staff use the student data collected for informing decisions on education policy the Student Data Access Policy and Procedures Guidebook was developed.

The goal of the Student Data Access Policy 4.300, Confidentiality of Individual Pupil Data and Data Redaction Policy 4.315 and this guidebook is to maximize access to the data we collect, while keeping the protection of student privacy as our top priority.

This guidebook has been developed by the Data Warehouse and Decision Support Team in conjunction with the DPI Data Privacy and Governance Committee (DPGC) and Data Privacy and Governance Workgroup (DPGW) to assist staff in properly protecting and handling student data while maintaining the confidentiality of the data.

Table of Contents

Acknowledgement

While developing the Student Data Access Policy 4.300, the Confidentiality of Individual Pupil Data and Data Redaction Policy 4.315 and this guidebook, the following resources offered invaluable guidance.

The U.S Department of Education and the Family Policy Compliance Office (FPCO) disseminate current information on the privacy rights of parents and students. The FPCO recently produced a Guidance for Reasonable Methods and Written Agreements which explains the exceptions under the Family Educational Rights and Privacy Act (FERPA). "The general rule under FERPA is that Personally Identifiable Information (PII) from education records cannot be disclosed without written consent. However, FERPA includes several exceptions that permit the disclosure of PII from education records without consent. Two of these exceptions are discussed in this document – the studies exception and the audit or evaluation exception. The two exceptions contain specific, and slightly different, requirements, described more fully in the implementing regulations (34 CFR Part 99)."

Other resources that provided guidance for this document are the National Center for Education Statistics (NCES) and the FORUM ("a diverse group of representatives from state and local education agencies [appointed by their state's superintendent]"). They developed a guide on student privacy: Forum Guide to Protecting the Privacy of Student Information: State and Local Education Agencies, NCES 2004-330. Washington, DC: 2004. The forward of the guide states, "The primary purpose of this document is to assist state and local education agencies to develop policies and procedures to protect information about students and their families from improper release, while satisfying the need for school officials to make sound management, instructional and service decisions."

Finally the Privacy Technical Assistance Center (PTAC) resources also informed the writing of this guide, Policy 4.300 and Policy 4.315. PTAC was established by the U.S. Department of Education "as a 'one-stop' resource for education stakeholders to learn about data privacy, confidentiality, and security practices related to student-level longitudinal data systems and other uses of student data. PTAC provides timely information and updated guidance on privacy, confidentiality, and security practices through a variety of resources, including training materials and opportunities to receive direct assistance with privacy, security, and confidentiality of student data systems." The PTAC Toolkit is kept current for all stakeholders wanting to gain more information on student data privacy.

Purpose

The purpose of both the Student Data Access Policy 4.300 and the Confidentiality of Individual Pupil Data and Data Redaction Policy 4.315 is to inform DPI staff of the federal and state laws governing student data privacy and to ensure the confidentiality of the student data while facilitating access by authorized users of the data. Policy 4.300 provides the guiding principles for access of the student information and the procedures that delineate the measures used by the DPI to protect student data privacy and confidentiality. Policy 4.315 provides the guidelines that

must be taken before data is published to ensure no identifiable student data is contained in any reports, charts graphs, etc.

The state agency and school personnel are legally and ethically obliged to safeguard the confidentiality of student data.

This guidebook was developed to introduce the concepts of student data privacy and confidentiality in the federal and state laws, provide more details on the processes and procedures outlined in Policy 4.300, and to provide specific guidance on how these processes and procedures should be implemented. In addition, detailed examples of redaction rules are also included.

Legal Consideration

The Family Policy Compliance Office (FPCO) administers two federal laws that provide parents and students with certain privacy rights:

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that is administered by the Family Policy Compliance Office (Office) in the U.S. Department of Education (Department). FERPA applies to educational agencies and institutions (e.g., schools) that receive funding under any program administered by the Department. FERPA protects the privacy of student education records.

FERPA has legal implications for state and local policies and procedures that guide aspects of data collection and reporting activities:

- ➢ Rights of a parent to review education records maintained by state or local education agencies
- ➢ Procedures by which education records can be released and protected

The Protection of Pupil Rights Amendment (PPRA). (20 U.S.C. § 1232h. Regulations: 34 CFR Part 98) governs the administration to students of a survey, analysis, or evaluation that concerns one or more of the following eight protected areas:

1. Political affiliations or beliefs of the student or the student's parent;
2. Mental or psychological problems of the student or the student's family;
3. Sex behavior or attitudes;
4. Illegal, antisocial, self-incriminating, or demeaning behavior;
5. Critical appraisals of other individuals with whom respondents have close family relationships;
6. Legally recognized privileged or analogous relationships, such as those of lawyers, physicians, and ministers;

7. Religious practices, affiliations, or beliefs of the student or student's parent; or,
8. Income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such program).

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 Wisconsin State Pupil Records Law (s. 118.125, Wis. Stats.) applies to school districts; portions also apply to DPI.

Student educational data should only be disclosed to those with legitimate educational reasons consistent with state and federal law. Furthermore, DPI believes that 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 non exhaustive list of federal and state laws govern the protection and privacy of student records and education data:

Federal Laws

1. Children's Online Privacy Protection Act (COPPA)
2. The Family Educational 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)

Personally Identifiable Data

The Department of Public Instruction and parents share a common interest in ensuring that personal information about children is kept confidential. It is important that department staff understand the concepts of personally identifiable and confidential data. Following are

definitions for key terms on the topic of confidentiality and the specific data identified by the department as confidential.

In general, personally identifiable data are data that contain information that would make the student's identity easily recognized. Release of this type of data is subject to state and federal laws and to the DPI Student Data Access Policy 4.300 and the Confidentiality of Individual Pupil Data and Data Redaction Policy 4.315.

The following are general concepts concerning individual information and privacy:

- Personal or individual information refers to information about a single individual;
- Personally or individually identifiable information reveals an individual's identity;
- Data confidentiality refers to an obligation not to disclose or transmit information to unauthorized parties;
- Privacy reflects an individual's freedom from intrusion;
- Indirect disclosure can occur when a single individual can be identified within a group because the data are reported by a combination of several identifiable characteristics and the group is small or when comparison of a combination of reports reveals identity.

NCES Discussion of Personally Identifiable Data

Personally identifiable data may or may not identify a person directly, but contain information that would make students' identities and any related information about them easily recognized. This information is more sensitive than grouped information or summarized data and therefore requires more attention and care before release. Personally identifiable information, including the identifying data listed below, must be maintained in education records that are protected with appropriate security. It is important that state or local education agencies establish policies that define personally identifiable information and list specific examples. This will avoid confusion when actual information requests are handled.

Personally identifiable data include *identifying* data that directly associate with a person, such as the following:

- A person's name;
- The name of the student's parent or other family members;
- The address of the student's parent or other family members;
- The telephone number of a person;
- A photograph of a person;
- An identifier, such as a person's social security number or an identification number assigned by the school [in Wisconsin, the Wisconsin Student Number (WSN) is considered confidential];
- A list of personal characteristics (e.g., apparent disability, a birthmark, or race and ethnicity) that would make the person's identity easily traceable;
- Other information that would make the person's identity easily traceable.

DPI List of Confidential Data

In November of 2003, the Office of Legal Services at the department categorized data that are confidential

C = Confidential

C Wisconsin Student Number (WSN) - *added in April 2006*
C Attendance
C Habitual Truancy
C Suspension
C Expulsion
C Dropout
C Course-Taking
C Retention
C Wisconsin Student Assessment System: (Wisconsin Forward Exam, Dynamic Learning Maps (DLM), ACT Aspire, ACT + Writing, ACT WorkKeys, Phonological Awareness Literacy Screening (PALS), ACCESS for ELLs, Alternate ACCESS for ELLs, National Assessment of Educational Progress (NAEP), etc.
C Primary Disability Category
C Migrant Status
C Homeless Status
C English Language Proficiency Level
C Educational Environment – *added in January of 2007*
C Free and Reduced Lunch Eligibility Status
C Social Security Number*****

N = not confidential

N Graduation
N Post-graduation Intentions
N Extracurricular and School-Sponsored Community Activities

*****The SSN is not collected in the Individual Student Enrollment System nor is it collected in the Wisconsin Student Locator System. It may not be used as an ID.

Wisconsin Law on Social Security Number
In 1997, s. 118.169, WIS. Stats. was enacted; this state law prohibits the use of the SSN as an unique student identifier.

Federal Law on Social Security Number
The Privacy Act of 1974 restricts the collection and use of SSN for everyone.

Directory Information

A general discussion of directory Information can be found in the following U.S. Department of Education publication:

National Forum on Education Statistics (2006)
Forum Guide to Privacy of Student Information: A Resource for Schools (NFES 2006-805).
U.S. Department of Education. Washington, DC: National Center for Education Statistics

Directory information is defined and the responsibilities of schools regarding that information are explained:

Directory Information
The term "directory information" is used for the portion of the education record that, if disclosed, would not generally be considered harmful or an invasion of privacy (34 CFR § 99.3)*.
This may include the student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance.

School systems should give careful consideration to designating data as "directory information" because once this designation is given, school officials may distribute the information to anyone who requests it, in or outside the school.

School systems that disclose directory information must give "public notice" of this policy and explain what is included in such information. The notice must also indicate that parents may refuse to allow the school to designate any, or all, of their child's record as directory information.

*The Family Educational Rights and Privacy Act Regulations (FERPA) 34 CFR Part 99 can be found at http://www.ed.gov/policy/gen/reg/ferpa/index.html

Within the regulations, Directory Information is defined as follows:

(Authority: 20 U.S.C. 1232g (a) (5) (A))
"Directory information" means information contained in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed. It includes, but is not limited to, the student's name, address, telephone listing, electronic mail address, photograph, date and place of birth, major field of study, dates of attendance, grade level, enrollment status *(e.g.,* undergraduate or graduate; full-time or part-time), participation in officially recognized activities and sports, weight and height of members of athletic teams, degrees, honors and awards received, and the most recent educational agency or institution attended.

Wisconsin Pupil Record Law
s. 118.125 (2) (j), Stats. also requires that schools give parents/guardians an opportunity to restrict access to directory information.

The department does collect a subset of directory information in the Wisconsin Student Locator System (WSLS) which assigns the Wisconsin Student Number (WSN), this is necessary to uniquely identify the students in the state. **In the 2015-16 school year the WISEid application will take over assigning the unique student number for choice and private school students, and in 2016-17 for public school students, and which time the WSLS system will be retired. The WSLS is currently used to:

1. Assign new WSNs to students entering Wisconsin Public Schools,
2. Help ensure that the WSNs stay with students as they move from school to school and district to district,
3. Update WSLS data such as when students exit a school or when data used for matching change (e.g. legal name, guardian), and
4. Correct errors in WSLS birthdates, spellings, etc.

The WSLS contains personally identifiable data such as student name, birth date, birthplace and parent's name and the WSN, access to this sensitive data is unconditionally restricted by policy 4.300 to the locally authorized staff of the individual school districts or 2r charter schools that provided the data and a minimal number of staff employed by the department or under contract to the department to solve technical issues with the data.

To provide an added measure of confidentiality for the individual student data stored at the department, the data in the WSLS system are stored separately from the individual student data systems such as the ISES system. In the ISES system the WSN is encrypted when viewed at the department. School district and 2r charter school staff may view the original WSN.

Department staff cannot link the ISES encrypted ID back to the original state assigned WSN without access to secured database functions within software managed by the department Database Administrator.

The WSLS was implemented using a "no release indicator" so that the WSLS can honor parent/guardian requests made to schools under FERPA 34 CFR Part 99 and s.118.125 (2)(j), Stats., for no-release of their child's directory data. If "no release" is indicated, then the WSLS restricts access to this student's directory data by WSLS users.

For a more detailed discussion on the "no release indicator" in the WSLS, see FAQ about WSLS No-Release Indicator.

What are Non-personally Identifiable Data?

Non-personally identifiable data do not reveal specific information about a particular individual. They usually describe a group of persons (e.g., the aggregate number of students participating in extracurricular activities) without identifying any one student. Or, they consist of individual records stripped of any information that would make it possible to identify the person described. Release of non-personally identifiable data is generally allowed (a good example of this is to look at the data reported on the public WISEdash pages). A district or school may determine

how this type of information is released. However, it is advisable to designate appropriate officials within the agency to review the compiled data, making sure that no single individual can be identified by a combination of several pieces of non-personally identifiable information. The Data Warehouse and Decision Support Team in the Division for Libraries and Technology provides guidance on how to appropriately safeguard personal information when publishing and sharing student educational information.

For instance, in reporting test scores for certain racial or ethnic groups in a school, if a school has only one student in a particular racial or ethnic group at a certain grade level, then that student's score could be made public by combining two separate pieces of information. It is important to be aware of the possibility of inadvertently disclosing personally identifiable information even when there is more than a single record in a category.

DPI has put in place redaction rules to ensure appropriate disclosure avoidance measures are taken when data will be made public. Disclosure avoidance involves a statistical technique to manipulate the data prior to release to minimize the risk of inadvertent or unauthorized disclosure of personally identifiable information. Specific guidance is provided for in DPI policy 4.315 *Confidentiality of Individual Pupil Data and Data Redaction*. The Division for Libraries and Technology provides specific guidance for ad-hoc reports that may be created within various business areas within the department.

Policy 4.300 restricts access to the individual student data and aggregate student data that may be identifiable, exclusively to the following 3 groups:

1. **Staff employed by or under contract to the Department of Public Instruction** must receive authorization to access individual student data and/or aggregate student data that may be personally identifiable by their immediate supervisor. 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 Policy 4.300 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. **School districts and 2r charter schools** where the student is enrolled*.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. Further detailed authorization steps are outlined in Policy 4,300.

3. **Parents and Eligible Students** as defined by Family Educational Rights and Privacy Act (FERPA). FERPA. (34 CFR § 99.3) 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.

NOTE:
The department will not permit access to, reveal, release, transfer, disseminate, or otherwise communicate all or any part of any individual student record or aggregate student record that may be personally identifiable orally, in writing, or by electronic or any other means to any person or entity except to properly authorized members of the above three groups.

*Enrolled student - for purposes of policy DPI 4.300 an enrolled student is receiving educational services directly from the district or from a 3rd party provider under the supervision of the school district. The district must submit records for enrolled students.

Confidentiality of Individual Pupil Data and Data Redaction Policy 4.315 protects the confidentiality of the data in public reporting.

In the Forum Guide to Protecting the Privacy of Student Information: State and Local Education Agencies the overview on privacy law indicates that each public agency should have one official who is responsible for ensuring the confidentiality of any personally identifiable information held at the agency and should train all persons who are collecting or using personally identifiable information regarding the state's policies on confidentiality and FERPA. At DPI, the people responsible for ensuring PII confidentiality and training is the Student Data Privacy Coordinator and the Data Privacy and Governance Workgroup.

Key Points for state agencies:

• FERPA privacy protections apply to student education records, all FERPA provisions apply to other education institutions and schools that receive funds from the U.S. Department of Education.

• FERPA establishes broad privacy protections for education records.

• FERPA grants parents and eligible students' access to education records,

• School districts and state agency written privacy policy ensures the uniform application of FERPA.

The DPI Student Data Privacy webpage contains additional valuable information about student privacy and data confidentiality. Staff receiving authorization to access student information are encouraged to access the website and review the material.

Why and How DPI Disseminates Secure Student Data

Why DPI collects data

DPI collects data to meet all required school, district, state, and federal reporting mandates, e.g.,

Every Student Succeeds Act (ESSA) (formerly ESEA), Individuals with Disabilities Education Act (IDEA), and Title II Higher Education Act. These data inform education research and data analysis. Through the DPI dashboard and reporting tools, DPI staff, teachers, administrators, parents, and researchers are better able to understand and improve educational outcomes for Wisconsin students.

DPI's Statewide Longitudinal Data System (SLDS) is titled the Wisconsin Information System for Education (WISE).

How the DPI Disseminates Secure Student Data

WISE

WISE is a comprehensive information system comprised of multiple tools that support data collection to meet all required district, school, state, and federal reporting mandates. Collected data are made available through "dashboards" (i.e., visual collections of graphs and tables) and reporting tools which inform education research and data analysis to better understand and improve educational outcomes for Wisconsin students. These tools promote high data quality, provide security procedures, and establish standards to ensure data privacy.

WISEdash Public Portal

The WISEdash Public Portal is a data portal that uses dashboards to provide multi-year education data about Wisconsin schools. Data on the portal are redacted and available by school, district or state. Redaction protects personally identifiable information. Up-to-date current and certified "snapshot" data can be displayed for multiple years and can be grouped and filtered by a variety of demographics including grade level, gender, race/ethnicity, economic status, disability, English proficiency, and migrant status. Data download files are also available. As a public reporting tool, WISEdash is used by districts, schools, parents, researchers, media, and other community members to view data published by DPI.

WISEdash for Districts

WISEdash for Districts, launched in September 2012, is a secure portal. To use this secure, password-protected portal, DPI has provided districts with flexible options for defining user roles when accessing the data. Role assignments by staff are determined by the districts to allow them to maintain local control of the implementation of the security and to ensure that the implementation is in line with current district policy. Roles include:

- **Summary Analyst Role** – Summary role of access to aggregate-level student data. Restricts access to individual student data.
- **Student Detail Analyst Role** – All permissions included in Summary Analyst Role plus the ability to drill down to individual student-level data with the exception of student-level socioeconomic status data.
- **Economic Indicator Analyst Role** – All permissions included in Student Detail Analyst Role plus access to student-level socioeconomic status information.

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

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.

Data Collection Process

The DPI has implemented rigorous authentication and authorization procedures to the data collection process. There are various data collections that are administered by numerous teams at DPI. All data collections meet a specific need, and must comply with federal and state laws that require such reporting.

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.

Technical Measures

Technical measures have been 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.

Breaches in Security

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.

The DPI Data Incident Response Plan can be found on the DPI intranet at the following network location. H:\LONGTERM\IT\Data Governance\Internal DPI\Data Management\Data Breach

Data Redaction for Data Requests and Public Reporting

Data Redaction is the process of masking the data displayed (e.g., 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 Confidentiality of Individual Pupil Data and Data Redaction Policy 4.315.

General Redaction Policy

The 4.315 Redaction policy addresses two interests:

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

In order to achieve a healthy balance between the privacy of students and the usability of education data, there needs to be consistent application of redaction criteria in all public reports that are generated at DPI. With that consideration there are primarily 2 different products to which redaction needs to be applied; public reporting dashboard applications and ad-hoc reports that are generated on an as needed basis.

DPI specific Tools and examples

The following section refer to examples of reporting that are specific to the products developed and maintained by the DPI.

Examples of redaction within DPI applications and tools

1. District and School Report Cards http://dpi.wi.gov/accountability/report-cards
    a. To protect student privacy, data for groups of fewer than twenty (20) 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 has "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 5 of the report card document or in DPI's School and District Report Cards Frequently Asked Questions documentation which can be found on the DPI web site: https://dpi.wi.gov/sites/default/files/imce/accountability/pdf/Report%20Card%20FAQ%202014.pdf

2. WISEdash Public Portal http://wisedash.dpi.wi.gov/
    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, which masks potentially identifiable variables.
    c. More information regarding direct/indirect disclosure and data redaction in the WISEdash Public Portal can be found on the DPI web site under the "Redaction" topic: http://dpi.wi.gov/wisedash/help/redaction**.**
    d. Examples of data suppression in the WISEdash Public Portal can be found on the DPI web site at: http://dpi.wi.gov/wisedash/help/no-data-graphs.
    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 on the DPI web site at: http://dpi.wi.gov/wisedash/help/glossary.

3. School District Performance Report (SDPR) https://apps2.dpi.wi.gov/sdpr/spr.action
    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. School level suppression shall be used to ensure that complementary disclosure avoidance techniques prevent direct and indirect disclosure for categories of reported data where enrollment/count is smaller than six. Additional steps shall be taken to suppress the next smallest categories when the sum of those suppressed enrollment counts are between 1 and 5.
    c. Some school districts have only 1 school, so school level suppression shall be transferred to district level suppression in these cases.
    d. District level suppression shall incorporate the same safeguards as school level suppression. Additionally, suppressed categories shall be counted. If the sum of the suppressed enrollment/count is between 1 and 5, or the count of suppressed categories = 1; then suppress the next smallest category that hasn't already been suppressed, or if tied for smallest, all tied categories shall be suppressed.

Examples of redaction in Ad-Hoc reports

1. Other Software Applications and/or Ad Hoc Data Requests
    a. Teams creating software applications that need to display redacted data shall ensure that redaction is designed and engineered into the application. The Division of Libraries and Technology provides guidance to software application development staff on these procedures.
    b. Teams who publish reports or data files on their own shall ensure that the report and/or data file is redacted. Because redaction is a complicated topic, the Division of Libraries and Technology should be consulted for guidance on redacting specific public reports.

i. Specific redaction rules that shall be applied to ad-hoc reports must include;
   1. When reporting whole numbers;
      a. Minimum Cell Size Redaction n = 20
         i. Replace cells less than 20 with an asterisk (*).
      b. Complementary Suppression - (In the event 1 cell is redacted, you must redact the next smallest cell so that any fields that display a total will not reveal the value of the redacted cell.)
   2. When reporting percentages; using a percentage when reporting data is common, however, a percent is a rate, number, or amount in relation to a whole. So when a percent is displayed with a total, you can determine the whole number value of that percentage, which could lead to overtly identifying the data that has been reported. When reporting in percent (%) you must consider the following safeguards for the reported data.
      a. Blurring/Rounding - Instead of using exact % round up to the nearest whole number %, or if using a small group, round to the nearest 5%.
      b. Top and Bottom Coding - any reported percentages that fall <5% or >95% can be reported as such. (E.g. 2.7% of students in a cohort of 37 = 1 student, so report it as <5%, which would equal 1.85 students.)

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. **In the 2015-16 school year the WISEid application will take over assigning the unique student number for choice and private school students, and in 2016-17 for public school students, and which time the WSLS system will be retired. 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.

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 individual's 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.

To use DPI applications that require a WAMS ID, you will need to perform the following process to get access:

1. Create a WAMS ID through the WAMS Self-Registration Process. **Use your DPI supplied email address in the WAMS email address field** when creating the WAMS ID profile.
2. 2, Provide the WAMS ID you created in the request process for application access.

External Access - School District and 2r Charter Schools

The School Districts and 2r Charters will follow the system they are currently using, the WAMS system.

1. Data Access is a role-based security system requiring user authentication and authorization.

2. The school district administrator is authenticated by DPI. All access is logon and password protected. DPI meets industry standards for a secure technical architecture.

3. The DPI develops and manages the data access roles which authorize access to specific information in student data bases. Access to administer specific tools with district data are authorized by the District Administrator or his designee.

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.
3. 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.
    a. 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.
    b. 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.

   c. 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.
4. 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.
5. 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)
6. The first time and every 90 days the local school staff use the data access software, they are required to agree to the following:
   a. I will respect and safeguard the privacy of students and the confidentiality of student data.
   b. I will comply with state and federal privacy laws and all district regulations, policies, and procedures established to maintain the confidentiality of student data.
   c. I will not disclose or transmit confidential data to persons not specifically authorized access to these data by the district WSLS/ISES Administrator, superintendent, or school board.
   d. I will use the confidential data for legitimate educational purposes only as necessary to perform my district-assigned tasks.
   e. I understand that my password is as important as my signature. It is my obligation to keep my password confidential. I will not share my password with anyone.
   f. I will not use other users' login names or passwords.
7. Local school district staff with the proper roles can access WSLS and educational progress data for their specific district in the various data bases/data warehouse at the department. The WSN is not encrypted when accessed by local school district staff where the student is enrolled.

Internal Access and Use of Data

Overview

At DPI we have many different locations where data is stored and various tools to access the data. Which database and/or tool you gain access to be determined by the data needed and the level of access needed to complete data analysis based on tasks performed and job functions determined by your manager.

Overall you will either access data through one of the following methods:

1 Direct database login with a User ID and password provided by the Database Security team for the database. (ISES application database, LDS ODS, Edvantage)
2 WAMS ID and password login to access DPI applications (see Wisconsin User ID below for information regarding a WAMS ID):
    a Data collection applications (WSLS/ISES).
    b Secure Home to access Application Security Manager assigned applications (WISEdash, MDAT, and SAFE).
3 LAN login for secured folders.

Role Based Data Access Method

All database, data systems, dashboard and reporting tools will utilize role based security. The role based security method provides authorization to software and databases through predefined access roles. In a role based security system, rules are developed that can provide access to the data at many levels, For example, one role may have rules that allow access to all the data in an entire database while another role may have rules that only allow access to view one field in one column in specified rows. This provides for security while being very flexible.

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.

Internal DPI Employee Data Access

1. Internal Data Access Request Process

The DPI developed the Internal Data Access Request Process 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.

Step by Step Process Instructions.

1. A legitimate need for data access to perform analysis and research. If student level data access is needed be prepared to provide the reason you need student Level data in the request.
2. Perform required Student Confidentiality Training.
3. Instructions for access to Application Databases and Tools.
    a. Review Data Access Request process to determine which security role will best suit the access to perform your data access needs.
    b. If the request is for Application Tool security, continue reading the instruction below; otherwise skip this step and go to step c.

i. 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. Self-Registration allows you to create **your personal** Wisconsin Login Account.
ii. If you do have a WAMS id, go to step c.

c. Create a Data Access Request Ticket in Footprints to initiate the Workflow Approval process Footprints Create Data Access Request.
d. The Request ticket will be sent to the Workflow Approval process for Approval or Disapproval of the request.
e. If the request is Approved by the Program Area AND the necessary DPI administrators:
   i. Request Ticket will be "Assigned" to a resource to add the security requested.
   ii. Assigned resource will update and close the ticket and an email will be sent to the Requestor.
f. If the request is Disapproved by either the Program Area OR necessary DPI administrators;
   i. Request Ticket will be closed.
   ii. An email will be sent to the Requestor explaining the Disapproval.

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.

5. Secure Home, Dashboard and Reporting Tools

To access Secure Home and the tools DPI has made available for data analysis a user must also have a WAMS ID. Once a user has a WAMS ID, access is granted through an application called Application Security Administrator (ASM). Roles have also been defined for these tools.

6. Direct Database Access

Data analysts can also request direct database access to specific databases and/or data to create custom sql queries for analysis. For direct access to databases, users need will receive access after approval and

- Oracle a separate username and password will be created by the DBA once the Internal Access Request has been received and approved.
- SQL Server the Active Directory username and password will be used. Access to student identifiable data will be reviewed closely before access is approved and granted.

7. Microsoft Access Database Tables

Some student data resides in Microsoft Access Database Tables. To access the Microsoft Access data, the requestor completes the Student Data Access Procedures (see page 16) and the Program Area Supervisor informs the program area staff that person may be granted access to the Microsoft Access tables or may access the Microsoft Excel subset files (see File Sharing below for the proper method of transferring the Excel files).

Staff that maintains the Microsoft Access Database Tables will not grant access to the Access Tables containing confidential data without the approval of the Program Area Supervisor. The Program Area Supervisor will email the staff in charge of the Microsoft Access Database Tables indicating that access should be granted. The staff will maintain the emails as a record of authorization.

8. Flat Files

Flat Files are files that are not within a database structure and include ASCII delimited files and Microsoft Excel files. Flat files with individual student data or unredacted aggregate student data may only be accessed by authorized individuals following the proper Student Data Access Procedures. (See page 15).

Once the procedures have been completed, the appropriate staff is granted access to the restricted, secured student data file sharing folder on the network. These folders are restricted to authorized groups. These folders can only be accessed if the staff have been authorized and added to the members of the appropriate group. Access through group assignment is provided through the Data Access Request on Fred. The LAN Administrator will be notified of the request and indicate staff have authorization to access data, the LAN Administrator will enter the staff into the group and save the email for record.

An example of use of flat files that may occur is the verification of school district truancy figures. The department calculates truancy from data collected in School Performance Report data collection and the data are stored in the Oracle database. The access is not through WAMS. To verify truancy data, staff may develop Excel spreadsheets of data containing two years and compare the current year to the last year as a logical edit of the data. If the change in the comparison is greater than some percent, the school district would be called to verify their submission.

If these truancy spreadsheets are based on unredacted data, the files will be stored in secured folders on the network. Any additional files generated from these files also would be stored on the network in the secured folder. Only staff with authority to access unredacted truancy data would have been given access to these folders by the LAN administrator. See Best Practices for File Handling Below.

Any paper reports generated from these truancy data must be stored in locked cabinets. The reports must be shredded when no longer needed.

The files would be deleted when the comparison edits were completed.

Best Practice File Handling of Flat Files with Individual Student Data

Staff granted access to the data within the secured folders must save additional work-generated files to the same secured folder. No files generated from the files in the secure folder may be saved to the staff's c: drive or any other drive on the LAN. The only allowed place of storage for these data and files are within the secured folder.

Files with individual or unredacted student data may only be shared within the department with staff and/or DPI contractors authorized for access to the specific data. The DPI Data Governance Coordinator keeps track of data access authorization and will be able to assist in identifying staff authorized for access.

- ➢ Files may not be shared outside the department without expressed permission of the Data Request Review Board.
- ➢ Files may never be taken home. The files must not leave the department's secure file structure.
- ➢ Files may not be sent attached to an email or within the body of an email unless the email is secured and encrypted.
- ➢ Files may not be copied to a CD or DVD or disk or any other media without the expressed authorization of the Data Request Review Board.
- ➢ At completion of a project, the student data files must be deleted subject to record retention rules, and federal and state requirements for data destruction.

The files are required to be stored on the network drive in secured folders, per backup policy procedures, the files will be backed up and although they may be deleted on the network drive, they will be saved in backup form per the department backup schedule. [The department backup schedule is reviewed and approved by the Legislative Audit Bureau in their annual audit of department procedures.]

Instructions for Flat Files

1. Student data must be stored in a secured restricted folder.

   a. Only those individuals authorized to access the specific files, shall have such access
2. Review section "Best Practice File Handling of Flat Files with Individual Student Data" on page 24.
3. Contact the Chair of the Data Request Review Board: with an email and specify the reason and duration of the requested access.
4. If the request is Approved by the Chair of the Data Request Review Board:
   a. The Chair of the Data Request Review Board: will email the LAN Administrator the staff is approved for authorization to access data in the restricted folder.
   b. The LAN Administrator will enter the approved staff as a member of the authorized group for the restricted folder and maintain the email approval as a record of authorization.
5. If the request is Disapproved by the Chair of the Data Request Review Board:
   a. The Chair of the Data Request Review Board: will contact you with the reason for disapproval.

9. Backup Schedule:

1. Backups of all files on the DPI LAN are taken nightly and kept until after the weekly backup.
2. A weekly backup is taken on Friday and kept until after the Monthly backup.
3. A monthly backup is taken on the last Friday of the month and is kept for one year.
4. An annual backup is taken on June 30th and kept for 7 to 10 years depending upon the record retention rules.

10. Paper Files

All paper files with individual student data or aggregate student data that have personally identifiable information must be stored in locked cabinets. Destruction of the files when no longer needed should be accomplished with a shredding machine.

The paper documents with individual or unredacted student data may only be shared within the department with staff and/or contractors authorized for access to the specific data.

Standard Student Data Access Procedures

Parent and Eligible Student Access

The Family Educational Rights and Privacy Act (FERPA) requires school district personnel to provide individual student data 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.

Non-Public Data Requests / Confidential Data Requests

1. Disclosure of Personally Identifiable Student Data

a. 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:
b. Staff employed by or under contract with DPI,
c. School district(s) where the student is currently enrolled,
d. Parents, legal guardians and eligible students,
e. Non-district personnel operating under appropriate institutional backing, within the limits of a binding DPI data use agreement, with legitimate educational interest as defined by FERPA. (34 CFR § 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 Educational 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. DPI enters into a written agreement that meets the requirements outlined below.

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.

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. Monitor 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.

DPI Staff Training

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

The Student Data Access Policy 4.300 included below delineates the measures the department has taken to protect confidential student data in the areas of data collection, security, and redaction in data displays, published reports or files.

The Student Data Access Policy 4.300 was developed to ensure the confidentiality of student data while maximizing the access to the information collected at the department. This policy covers the access to both the individual student data and to the aggregate student data that is not redacted and therefore may be personally identifiable.

Policy 4.300 covers external and internal access and use of student data by staff employed by and/or under contract to the department, the school districts and/or 2r charter schools where the student is enrolled and parents and eligible students.

The Department of Public Instruction and parents share a common interest in ensuring that personal information about children is kept confidential. In addition to this policy that focuses on student data access, the DPI follows a strict Confidentiality of Individual Pupil Data and Data Redaction policy 4.315 to ensure pupil confidentiality when data are reported publicly

DPI Data Privacy and Governance Structure

DPI Data Privacy and Governance Committee (DPGC)

- Establish Data Privacy and Governance Policies
- Establish Data Privacy and Governance Workgroup (DPGW)
- Resolve issues escalated by the DPGW
- Approve data policies & major data-related decisions proposed by the DPGW

- Hold program/agency areas accountable for adhering to the data governance and privacy policies

Name	Division	Team
Debi Townes	Finance and Management	School Finance
Tricia Collins	Finance and Management	School Management
Rebecca Vail	Academic Excellence	Content and Learning
Laura Pinsonneault	Student and School Success	Educational Accountability
Julia Hartwig	Learning Support	Special Education
Melissa Straw	Libraries and Technology	Data Warehouse and Decision Support
Kurt Kiefer	Libraries and Technology	Executive sponsor

Data Privacy and Governance Workgroup (DPGW)

Charge:

- Establish and document program standards, processes, and procedures for data collections, reporting, and release with consideration to the protection of privacy.
- Identify, prioritize, and resolve critical data issues affecting the quality, availability, or use of data
- Responsibility for professional learning and training
- Keeping up-to-date on privacy issues at the federal and state level;
    - PTAC guidance documentation
    - CCSSO EIMAC Data Privacy Workgroup
    - FERPA
    - COPPA

Name	Division	Team
Julie Palkowski	Academic Excellence	Content and Learning
Sarah Kolbe	Student and School Success	Educational Accountability
Nic Dibble	Learning Support	Student Services, Prevention and Wellness
Phil Olsen	Student and School Success	Educational Accountability
Paul Sherman	Learning Support	Special Education
Sean Cottrell	Libraries and Technology	Data Warehouse and Decision Support
Kathy Boguszewski	Libraries and Technology	Data Warehouse and Decision Support
Melissa Straw	Libraries and Technology	Data Warehouse and Decision Support
Kurt Kiefer	Libraries and Technology	Executive sponsor

Data Request Review Board (DRRB)

Charge

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

Name	Division	Team
Sean Cottrell	Libraries and Technology	Data Warehouse and Decision Support
Carl Frederick	Research Analyst	Policy and Budget Team

Resources

Colorado Department of Education; Data Privacy and Security Homepage

EdPolicy Leaders Online - Key Terms

Family Policy Compliance Office

Kentucky Department of Education Best Practice Guidelines

National Center for Education Statistics

Pennsylvania Department of Education Student Data Access and Use Policy

Privacy Technical Assistance Center (PTAC)

PTAC Case Studies

PTAC Written Agreement Checklist

U.S Department of Education

Virginia Longitudinal Data System Resources

Wisconsin's Data Breach Notification Law

Glossary of Terms

2R Charter Schools are the same as regular charter schools except that their authorizers are one of the following:

- The Common Council of the City of Milwaukee
- The Chancellor of the University of Wisconsin - Milwaukee
- The Chancellor of the University of Wisconsin - Parkside
- The Milwaukee Area Technical College District Board

All 2R charter schools are considered non-instrumentality schools since the above authorizes the governing board of the charter school to perform specified duties for the board of regents with respect to the instructional staff. This authorization may include duties related to supervising the instructional staff, taking disciplinary actions with respect to the instructional staff, recommending new hires or layoffs, collective bargaining, claims, complaints, or benefits and records administration.

For more in-depth information on 2R charter schools see: Wisconsin Legislature Chapter 118.40 quick reference or Wis. Stats. Chapter 118.40(2r).

Aggregated Student Data That Is Personally Identifiable – Student data that indirectly identifies a student. The Individual Student Enrollment System (ISES) data and other education progress data do not contain the student name; they do contain many disaggregated categories including but not limited to the student's gender, racial/ethnic category, disability status, economic status and English proficiency. Because the individual student data systems and the aggregate student data systems that may be personally identifiable contain so many disaggregated characteristics for each student,

there may be only one or a very small number of students with a specific set of characteristics in an entire school. A combination of information could indirectly identify a student; the department has enacted this access policy and set of procedures to ensure the confidentiality of the student information.

Following is an example of two student records with some of the disaggregated categories. Because of the detail of disaggregated characteristic stored about the students, one can see why counts of students can result in very small groups, fewer than 5 students, and could result in potential identification:

Encrypted Student ID	District	Sch	Grade	G	Race/ Ethnicity	Econ Disadv Status	Primary Disability	Sec 504	LEP	Migrant	Test Stat
y*^"o%q#b#	1234	123	4	F	H	F	LD	Y	N	Y	P
z*="r%'#b>|	1234	123	10	M	B	Y	SL	N	Y	N	T

Access - Viewing, editing, printing, downloading, copying, or retrieving data from a computer, computer system, computer network, or other medium.

Confidential Data - Personally Identifiable Information about a student that may not be disclosed without authorization in Federal and WI State Law.

Confidentiality - refers to your obligation not to disclose or transmit information to unauthorized parties. Confidentiality extends to information about either individuals or organizations. In schools, districts, or state education agencies, that usually means establishing procedures that limit access to information about students or their families. This access extends to the school officials who work directly with the students, agency representatives who serve as evaluators or auditors, or individuals who act on behalf of authorized education officials.

Data Confidentiality - refers to an obligation not to disclose or transmit information to unauthorized parties.

Data Governance - The roles, structures, and processes DPI uses to make decisions about data sharing, access, use, and privacy.

De-identified Data - Data that has been "anonymized" by removing all personally identifiable information, such as students' names, to protect personal privacy.

Disclosure (or Release) - includes permitting access to, revealing, releasing, transferring, disseminating, or otherwise communicating all or any part of any individual record orally, in writing, or by electronic or any other means to any person or entity.

DRRB - Data Request Review Board

Educational Environment - refers to the extent to which students with disabilities receive special education and related services in classes or schools with their nondisabled peers

Education Record – For purposes of this guidebook, an education record is any Personally Identifiable Information (PII) data regarding a student that is reported to, received by or maintained by the department. This includes, but is not limited to, a pupil's name, address, phone number and WSN, parent's name, address, and phone number. The form of the data covered includes, but is not limited to, electronic and hard copy. More information on Safeguarding Personally Identifiable Information refer to this Resource.

Education Record (NCES) - An education record is a compilation of records, files, documents, and other materials that contain information directly related to a student and maintained by education agencies or institutions, or by individuals acting on behalf of the agencies. According to FERPA, a record means any information recorded in any way, including, but not limited to, handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche. An education record, sometimes referred to as a student record, may include a variety of details about a student such as the date of birth, date of enrollment, bus route, immunization history, achievement test scores and grades, enrollment and attendance, awards, degrees achieved, and special education plans and evaluations. Personal notes by teachers or other staff that are not meant to be shared are not part of an education record. A record of a student may be maintained in more than one location within an agency or school (e.g., enrollment record in the school's administrative office and health information in the school health clinic).

Information included in an education record is collected primarily from the student (or family members), teachers, and other school staff. It may also be collected from other sources outside the school, such as health care providers or testing companies. Personal information about students is a vital resource for teachers and school staff in planning responsive education programs and services--designing individual education plans; scheduling students into appropriate classes; planning school bus routes; and completing reports for local, state, and federal authorities. In emergencies, the information is readily available to school officials to assist students and their families. A limited amount of this information, as defined by the school district or the state, makes up a student's permanent records or transcripts.

Eligible Student or Parent - FERPA grants parents the rights to review, request amendment to, and release education records. A parent means a natural or adoptive parent, a legal guardian, or an individual acting as a parent in the absence of the parent or guardian. These rights transfer to eligible students when they reach eighteen or when they attend a postsecondary education institution. However, parents can still have access if the eligible student is a dependent for tax purposes, unless the eligible student notifies the school district that the parents may no longer have access.

Enrolled Student - For purposes of this policy, a school district has to submit records of any student enrolled that is receiving educational services directly from the district or from a 3rd party provider under the supervision of the school district.

FERPA - Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) protects the privacy of student education records;

Flat Files - are files that are not within a database structure and include ASCII delimited files and Microsoft Excel files. Flat files with individual student data or unredacted aggregate student data may only be accessed following the proper Student Data Access Procedures.

Indirect disclosure – can occur when a single individual can be identified within a group because the data are reported by a combination of several identifiable characteristics and the group is small or when comparison of a combination of reports reveals identity.

Individual Student Data – Non-aggregated data collected at the individual student level.

ISES - Individual Student Enrollment System – The Individual Student Enrollment System (ISES) is used to collect confidential data about students as required to produce reports mandated by state and federal laws and allows educators to (1) better account for students who move or are highly mobile, (2) more readily exchange student records among school districts, and (3) respond more quickly to areas in need of improvement. ISES requires that schools and/or districts submit data on students enrolled during the previous school year and students enrolled on the current year count date. Districts submit a limited range of WSLS data (e.g. WSN, school, enrollment date) along with data required by ISES in order to verify the student's school enrollment status and WSN, but districts do not submit student names or other directory data as part of ISES. **In the 2015-16 school year the WISEid application will take over assigning the unique student number for choice and private school students, and in 2016-17 for public school students, and which time the WSLS system will be retired.

Legitimate Educational Interest – The legitimate educational interest of staff authorized to access student data will be determined on a case-by-case basis by the Assistant State Superintendent in whose division the data are collected and the Data Request Review Board. The following are examples of criteria that may constitute legitimate educational interest:

- The information requested is necessary for that staff to perform appropriate tasks that are specified in his or her position description or by a contract agreement.
- The information is to be used within the context of official agency business and not for purposes extraneous to the staff's or contractor's areas of responsibility to the agency.

- The information is to be incorporated into legitimate educational research purposes governed by a binding data use agreement with a comprehensive set of guidelines to ensure compliance with FERPA and Wisconsin Pupil Records Law (118.125).

NCES - National Center for Education Statistics

Unredacted aggregate student data - are data that have not been suppressed to protect pupil confidentiality. Aggregate (summarized) data may be personally identifiable if the cell sizes are small and there are identifying characteristics associated with the data.

Parent or Eligible Student - FERPA grants parents the rights to review, request amendment to, and release education records. A parent means a natural or adoptive parent, a legal guardian, or an individual acting as a parent in the absence of the parent or guardian. These rights transfer to eligible students when they reach eighteen or when they attend a postsecondary education institution. However, parents can still have access if the eligible student is a dependent for tax purposes, unless the eligible student notifies the school district that the parents may no longer have access.

Personal or individual information - refers to information about a single individual

Personally identifiable data - are data that contain information that would make the student's identity easily recognized. Release of this type of data is subject to state and federal laws and to the DPI student data access and reporting policies.

PII - Personally Identifiable Information - Any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to the individual.

PPRA - Protection of Pupil Rights Amendment

Privacy - The balance between collection and dissemination of data, technology, and individuals' right to have their personal information kept private.

PTAC - Privacy Technical Assistance Center

Security - The policies and practices implemented at the state, district, and school levels to ensure that data are kept safe from corruption and that access is limited and appropriate. Data security helps ensure privacy and protect personally identifiable information.

SPII - Sensitive PII - Personally Identifiable Information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Sensitive PII requires stricter handling

guidelines because of the increased risk to an individual if the data are compromised. (e.g. Wisconsin Student Number, Test Results (State Assessment, Alternative Assessment for Student with Disability) Advanced Placement, ACT ACCESS, etc.), Attendance, Habitual Truancy, Suspension, Expulsion, Dropout, Course-Taking, Retention, Primary Disability Category, Migrant Status, Homeless Status, English Language Proficiency Level, Free and Reduced Lunch Eligibility Status

SLDS - Statewide Longitudinal Data System - A data system that collects and maintains detailed, high quality, student and staff-level data that are linked across entities over time, providing a complete academic and performance history for each student; and makes these data accessible through reporting and analysis tools.

Student Data – For purposes of the Data Access Policy 4.300, student data is used interchangeably with Education Record.

WISEid - In the 2015-16 school year the WISEid application will take over assigning the unique student number for choice and private school students, and in 2016-17 for public school students, and which time the WSLS system will be retired.

WSLS - Wisconsin Student Locator System - The Wisconsin Student Locator System (WSLS) assigns a WSN to each student new to Wisconsin public schools and helps ensure that the WSN stays with the student as he or she moves from school to school and district to district. **In the 2015-16 school year the WISEid application will take over assigning the unique student number for choice and private school students, and in 2016-17 for public school students, and which time the WSLS system will be retired. WSLS contains personally identifiable data such as student legal name and aliases, birth date, one or more parent names, schools attended, and other information that is generally not considered harmful or an invasion of privacy. These personally identifiable data are used to facilitate the student matching process as students move within the PreK-20 system. All the data in WSLS, especially the WSN and the connection between the WSN and other personally identifiable data, are considered sensitive and access to these sensitive data is unconditionally restricted by this policy to a minimal number of staff employed by the department or under contract to the department to solve technical issues with the data. WSLS data are also accessible to locally authorized staff of the individual school districts or 2r charter schools that provided the data and, to the extent permissible by law, to locally authorized staff in other Wisconsin public schools for student matching purposes. WSLS data are stored separately from other student level data collected by the department through ISES and other systems.

WSN - Wisconsin Student Number – A unique, unduplicated number assigned to a student that has no embedded meaning and that remains with the student during his or her PreK-12 Wisconsin public and/or private school experience and transitions to the DPIs postsecondary partners. WSNs are not considered directory data and must be kept confidential. WSNs, in lieu of student names, are attached to a wide range of confidential student data to help protect student privacy and to facilitate reporting. WSNs are

encrypted in WSLS and ISES when stored with confidential student level data as an added measure to protect student privacy. The encrypted ID cannot be linked back to the original state assigned WSN without access to secured data base functions within software managed by the DPI Database Administrator. School district staff where the student is enrolled may view the original WSN.

Access to student data and statistical information summarized from the data are an important resource for the purposes of monitoring programs and evaluating education policies. Strong state and federal pupil records laws protect the privacy of students and their families. This policy was developed to ensure that these laws are not violated by the department.

Frequently Asked Questions (FAQ)

What do I do if a researcher, PhD candidate, social worker, staff from another state agency, staff from another state institution, staff from another state, or any other organization – profit or nonprofit, public or private calls and asks for access to confidential student information?

The DPI restricts access to confidential student data as described in Data Access Policy 4.300. The policy allows access only to authorized staff employed by or under contract to the DPI, parents and eligible students, and the locally authorized staff of school districts and 2r charter schools where the student is enrolled. Calls may be referred to the DPI Data Governance Coordinator.

What do I do if a parent or eligible student calls and asks to see their student's information?

When a parent calls asking to see their student's information, direct the call to the Chair of the Data Request Review Board. Parents have a right under FERPA to access their student's information; the Data Request Review Board or their designee will assist them with DPI procedures for access.

What do I do if a school or district staff calls and asks for access to student data?

There is a procedure for school district and 2r charter school staff to access their individual data. Their local School District Administrator and/or their designee authorize the staff using the Delegated Authority Application http://lbstat.dpi.wi.gov/lbstat_delauthapp or Application Security Manager (ASM) http://wise.dpi.wi.gov/wise_securehomeinfo. The requesting staff should contact their own District Administrator's office to gain access. Calls may be referred to the Chair of the Data Request Review Board or their designee.

What do I do if a newspaper or other media call and asks for access to student data?

All contacts from any media, TV, radio, newspaper, etc. are to be directed to the DPI Communication Office (currently Tom McCarthy).

Where do I access data about student enrollments for content areas?

Please submit a request on the DPI General Data Request pages found here, indicating the content area where enrollment numbers are requested. (http://dpi.wi.gov/wise/data-requests/general-data-request)

How do I securely exchange confidential student information with a district?

Typically, Accellion is the SFTP tool used to send and receive student data at DPI. When using email to discuss an individual student, it is recommended to use only the name of the student. If the issue requires additional identifiable information to ensure the correct student is being discussed, those details should be discussed over the phone, rather than including in email. Always be mindful of who you are sending data to and ask yourself, does this person really need this data?

You are encouraged to consult with the Division for Libraries and Technology - Data Warehouse Team for specific guidance on unique exchanges.