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

Subject	Effective Date	Index	Page
STUDENT DATA ACCESS	**04/01/16**	**4.300**	**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. 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).