



# Student Data Access and Use Policy

---

## **Purpose:**

Data on student status and performance linked to a random numerical identifier is collected by the Pennsylvania Department of Education (PDE) for the purposes of satisfying federal and state mandates and reporting requirements and improving education for all students in the Commonwealth. This collection of data is designated as the Pennsylvania Information Management System (PIMS).

The confidentiality of this data must be protected. Therefore, PDE will not release or disclose personally identifiable student level data regarding students in the public schools of Pennsylvania unless permitted by law.

The purpose of this policy is to prescribe how data will be collected, maintained and disseminated in compliance with applicable federal and state laws. This policy applies to all organizational units, their agents and staff within PDE, their authorized agents and any contractors, subcontractors and their agents.

PDE personnel with specific questions regarding the release of student information should direct those inquiries to the Office of Chief Counsel. Any other individual with any questions regarding student information or this policy should contact the Division of Data Services, Pennsylvania Department of Education.

## **I. Introduction/Background**

This policy statement pertains to individual student data collected and maintained by PDE. Individual student data are used for the purpose of collecting data needed for state and federal reporting, including the federal *No Child Left Behind Act*, state assessments, state aid, special education and program participation as well as to satisfy other data requests from PDE, the state legislature, and other authorized entities.

Individual student data are managed by PDE in accordance with state and federal laws. The Family Educational Rights and Privacy Act of 1974 (FERPA), 20 U.S.C. §1232g, and its implementing regulations found at 34 CFR Part 99, the Individuals with Disabilities Education Act (IDEA), 20 U.S.C. §1417(c), 1439(a)(2), and its implementing regulations found at 34 CFR § 300.123 and §300.622, and Pennsylvania statutes, regulations and policies govern the confidentiality of, and access to, students' educational records. This policy statement contains information about the procedures that will be used to ensure the confidentiality of student information and data maintained by PDE. This policy does not expand or in any way change the allowable uses by staff of these data or the availability of student data to any other educator or member of the public.

The student data collected in PIMS is intended to support better decision-making and policies for improving the performance of students and schools. PDE intends that PIMS will ultimately reduce the reporting burden, help to facilitate the entry of students into a new local education agency (LEA), and ensure that timely, high quality data are available to authorized users.

Data is collected on all Pennsylvania students in public schools, as well as students in participating private or nonpublic school entities. The data are collected periodically in a prescribed format and reflect what is needed for reporting and decision-making. Student data are consistent with best practice definitions as identified by state and national standards groups, such as the National Center for Education Statistics (NCES).

The Secretary of Education or his/her designee has the authority to establish a system that maintains data in accordance with FERPA and other relevant state and federal laws and regulations.

## II. Definitions and Background Information Related to this Policy

Pennsylvania adheres to the confidentiality requirements of both federal and state laws, including, but not limited to, FERPA, IDEA, the Protection of Pupil Rights Amendment (PPRA), the National School Lunch Act, and 22 Pa. Code §12.31-§12.32. The following definitions are derived from these laws and other related documents that are relevant to the implementation of this policy.

*Access* means viewing, editing, printing, downloading, copying, or retrieving data from a computer, computer system, computer network, or other medium.

*Confidential data* includes personally identifiable information about a student that is prohibited from disclosure pursuant to state or federal law or information that is intended for the use of a particular person/group and whose unauthorized disclosure could be prejudicial to the individual it identifies. **Information which allows for the** identification of an individual student and that is collected by PDE is considered personally identifiable information and may not be released without parental **consent**, except in very limited circumstances set forth in 34 C.F.R. §99.31. This information includes, but is not limited to:

- Family information such as names, address, phone numbers, personal and business financial data, household members' social security numbers, household members' employment information, household Temporary Assistance for Needy Families (TANF), Food Stamp eligibility.
- Personal information such as identification codes, grades, scores, courses taken, other specific information linked directly to a student
- Special Education records
- Free or Reduced Price eligibility status of individual students in USDA-funded school lunch, breakfast and milk programs, Summer Food Service Programs, and Child and Adult Care Food Programs.
- Information that would make the student's identity easily traceable.

*Confidentiality* refers to PDE's obligation not to disclose or transmit personally identifiable information about individual students to unauthorized parties. Confidentiality consists of the measures used to protect how personally identifiable information is collected and maintained

and when consent by the student or his or her parent/guardian is required to release information.

*Disclosure* means permitting access to, revealing, releasing, transferring, or otherwise communicating personally identifiable information contained in education records to any party, by any means, including oral, written, or electronic.

*Personally identifiable student level data and/or information* includes, but is not limited to: the student's name; the name of the student's parent/guardian; the address of the student or student's family; personal identifiers, personal characteristics or other information that would make the student's identity easily traceable.

### **III. Guiding Principles**

The following principles have been used in establishing this policy:

- Student information is a valuable asset and should be treated as such;
- PDE manages student information under its control throughout its life cycle, from original submission to appropriate destruction;
- PDE is responsible for managing appropriate access to and use of student information;
- Chief School Administrators are responsible for authorizing access to student information at the LEA level;
- PDE is responsible for reviewing and updating policies and regulations covering confidential student information and ensuring that its activities comply with state and federal law;
- PDE will make its student data access and use policy available to the public.

### **IV. Measures Used to Protect Confidentiality**

To ensure the maintenance of confidentiality of student data, this policy includes four privacy and confidentiality protections. These include assignment of a unique identifier, data security, restricted access and statistical security.

#### **Assignment of a Unique Identifier (PAsecureID)**

The PAsecureID is a ten digit number that is generated for each student, is unique to that student and will protect the confidentiality of the individual student record of each student. The PAsecureID database contains a selected set of data about individual students that will allow for the assignment of a unique student identifier. The PAsecureID is randomly generated and contains no embedded meaning. Once the number is created it is first checked for duplicates. If any duplicates are found, they will be reconciled using a set of information, such as the first name, last name, date of birth, gender, race/ethnicity, and the LEA identification number of the student. After being checked for duplicates, the number is made permanent.

There are numerous benefits which result from the assignment of a PAsecure ID. For example, upon receiving a student who has transferred into his/her LEA from another LEA within Pennsylvania, an LEA administrator must locate the student's unique student identifier and access personally identifiable information regarding the student. The goal of this system is to maintain a unique identifier for every Pennsylvania student such that: 1) only one student is ever

assigned a particular number; 2) once a student is assigned a number, that number is always associated with that student throughout his or her educational career or until he or she leaves the state; and 3) a student is only assigned one number so that the student is not duplicated when reporting to PDE.

## **Data Security**

Security includes the technical measures put into place by the Commonwealth of Pennsylvania to ensure that records are not lost, stolen, vandalized, illegally accessed, or otherwise rendered useless. Since the data are stored on computers there will be a high level of protection that provides integrity and availability commensurate with the level of risk and magnitude of harm. Procedures that will be used include secure firewalls, secure socket layers, audit trails and physical security, such as restricted server room access. All Commonwealth of Pennsylvania and federal security policies shall be followed and regularly audited.

## **Restricted Access to Student Level Data**

### **LEA and School Personnel**

The chief school administrator of an LEA or their designee is responsible for authorizing access to data concerning students enrolled in that LEA. An individual will be granted access to specific data upon signing an assurance statement and receiving approval of the chief school administrator or his/her designee.

### **LEA Access to PAsecureID**

PAsecureID allows LEAs to upload a batch file of their students, download a batch file of students previously submitted from their LEA, create a PAsecureID on-line, or use the search functionality to locate individual students. LEAs will only be allowed to view or download their own batch files. LEA staff may only use the search functionality for the purpose of locating students already assigned a PAsecureID.

### **PDE Staff Access**

PDE staff will have access to student level data on an individual basis only through a PAsecureID. No PDE personnel will have access to student names and individual state assessment test scores. The Data Base Administrator will have access to the entire database, but only for purposes of troubleshooting and correcting errors or avoiding potential errors. Any PDE employee or authorized agent assigned responsibilities that require student level data access must sign an assurance statement. Examples of staff requiring access are those who work directly with LEAs in implementing and supporting student longitudinal data systems and the technical staff required to support those systems. The specific level of access to student data depends upon the staff member's responsibilities. Other PDE staff will only have access to student data at an aggregate level.

## Other Access

Individuals, other than those listed above, will not have access to student level data, except under the circumstances listed below.

## Access Exceptions

Under this Policy, no personally identifiable student information will be released without the consent of the parent or eligible student except under the following circumstances as permitted by FERPA , as set forth in 34 C.F.R. §99.31:

1. To teachers and officials of the LEA in which the student is currently enrolled who have a legitimate educational interest in the information, under Section 99.31(a)(1), with the approval of the chief school administrator or designee.
2. To LEA and school personnel where a student seeks or intends to enroll, under Section 99.31(a)(2).
3. To comply with a lawfully issued subpoena or court order, under Section 99.31(a)(9)(i), following notification requirements set forth in Section 99.31(a)(9)(ii).
4. To educational officials in connection with an audit or evaluation of a federal or state supported education program, under Section 99.32(c)(3), subject to the requirements of Section 99.35.
5. To appropriate parties in connection with a health or safety emergency, if such knowledge is necessary to protect the health and safety of the student or other individuals under Section 99.36(a).

## Record of Access

The Secretary of Education or his/her designee shall maintain a record of each request for access to personally identifiable information regarding a student which is granted and of each instance where personally identifiable information is disclosed. This record shall include the parties who have requested or received personally identifiable information and the legitimate interests the parties had in making the request or in having been provided access. A record need not be maintained if the request was from, or the disclosure was to: (1) The parent or eligible student; (2) A school official or employee of the LEA in which the student is currently enrolled with a demonstrated legitimate educational interest; (3) A party with written consent from the parent or eligible student; or (4) A party seeking or receiving the records as directed by a Federal grand jury or other law enforcement subpoena and the issuing court or other issuing agency has ordered that the existence or the contents of the subpoena or the information furnished in response to the subpoena not be disclosed.

## Disclosures

Any release of personally identifiable information is subject to the following conditions: (1) the party to whom the data are released does not disclose the information to any third party without the prior written consent of parent or eligible student; (2) the data will be used only for the purpose for which the disclosure was made; and (3) the data are destroyed when no longer needed for the purposes under which the disclosure was granted.

## **Statistical Security**

PDE will use the student data to produce aggregate reports from individual data that relate to groups of students, rather than individual students. The student data will also be linked to other PDE databases to produce additional aggregate reports. While it may seem that the use of anonymous aggregated data poses little threat to confidentiality, there are some cases where specific populations may include only a few individuals. Statistical disclosure is the risk that arises when a population is so narrowly defined that tabulations are apt to produce a reported number small enough to permit the identification of a single individual. In such cases, the Secretary of Education will enforce statistical cutoff procedures using a minimum confidentiality  $n$  of 10 to ensure that student confidentiality is maintained. It is the intent of PDE to avoid the possibility of inadvertently reporting personally identifiable information about any student.

## **V. Data Use and Release**

### **State and Federal Reporting**

A key purpose of maintaining student level data is to provide access to statistical information that improves the education-related decisions of teachers, administrators, policymakers, parents, and other education stakeholders. Confidential data on an individual student will not be disseminated in violation of federal or state law. Furthermore, it shall not be used for any purpose other than those stated in this policy. If PDE enters into a contract with a private individual or third party to perform any of the data reporting or statistical analysis, that agreement shall require that the data be protected in the same manner. PDE will aggregate the individual student data to comply with required state and federal reporting.

### **Agency Data Sharing**

PDE has inter-agency agreements to share limited amounts of data for the benefit of the children of Pennsylvania, as allowed by law. All sharing of student data must comply with the requirements of FERPA. PDE will comply with requests for individual student data from federal and state governmental agencies as required by law.

### **Researchers**

#### **Aggregate Information**

PDE regularly responds to requests for aggregate student data by researchers. Aggregate data does not include any student specific information, including, but not limited to, name and student identifier. The Department will work with researchers with the goal that they receive the most meaningful data possible without the disclosure of information that would make any student's identity easily traceable.

#### **Personally identifiable information**

PDE also receives requests for personally identifiable information about students from researchers in many contexts. Since PDE acquires personally identifiable information from LEAs pursuant to Section 99.31(a)(3) of the FERPA regulations, the Department may not redisclose personally identifiable information to a third party researcher unless the researcher is

acting as an “authorized representative” of the Department acting under the direct control of the Department as an employee, appointed official or contractor who is providing services that the Department would otherwise provide for itself.

Likewise, Section 99.31(a)(6) permits information about individual students to be released without parental permission to researchers conducting studies for or on behalf of the Department to develop, validate or administer predictive tests; administer student aid programs or improve instruction. In order to permit a release of personally identifiable information under Section 99.31(a)(6), the Department must have authorized the study and it must be conducted for or on behalf of the Department. The fact that an outside entity, on its own initiative, conducts a study which may benefit an educational agency or institution does not transform the study into one done “for or on behalf of” the Department.

Beyond these limited circumstances, personally identifiable information about a student may not be provided in response to research requests. Researchers must submit a written request for any data to the Secretary of Education or his/her designee. The request must explain the purpose of the research study, the facts that demonstrate that the Department authorized the study or that the study is being conducted on behalf of the Department, and how the researchers will ensure data confidentiality and security. This includes how the data will be stored, used, maintained, disseminated and destroyed. Requests will be considered on a case-by-case basis to determine if they are in compliance with state and federal laws and regulations. Any release of student data to researchers outside PDE is considered a loan of data, i.e., the recipients do not have ownership of the data. Researchers will be required to supply a copy of any analysis or reports created with the data and to destroy the data once the research is completed. PDE reserves the right to charge a reasonable fee for the use of data by researchers to help offset the state’s costs of collecting and storing the data.

## **Parents**

Upon request, and as specified under Section 99.10(a)(2) of the FERPA regulations, the Secretary of Education or his/her designee will provide access to a student’s education data to a parent, legal guardian or the student if the individual is over the age of eighteen. Such access must be provided within 45 days of a request. If the education data contains information on more than one student, the parent or eligible student may inspect and review or be informed of only the specific information about that student.

## **VI. Improper Disclosure of Student Records**

The Secretary of Education or his/her designee has the responsibility for determining whether a request for access to student records constitutes a legitimate request for an appropriate usage of student data. If the request does not meet standards established by PDE for the lawful release of student data, then the Secretary of Education or his/her designee will deny the request.

The Secretary of Education is also responsible for determining if personally identifiable or confidential information has been inappropriately disclosed by a PDE employee or authorized agent in violation of this policy. Such disclosure, which may constitute a violation of federal law, may be subject to a disciplinary action, including termination (if a PDE employee), or suspension of login privileges. If an improper disclosure is made by someone other than a PDE employee or authorized agent, then the involved parties will not have access to any student data for five years.

## **VII. Ownership of the Data**

LEAs or other primary sources of the data that are located at PDE are the originators and owners of those data. The Secretary of Education functions as the custodian of the data in PDE. In order to protect the data in its custody, PDE has established this policy that is implemented by the Secretary. The policy ensures that all data are securely maintained with safeguards on all personally identifiable or confidential information.

# Student Data Non-Disclosure Agreement

---

Individual student information maintained in the Pennsylvania Information Management System is collected for the purpose of meeting local, state and federal reporting requirements. The data are protected by state and federal laws and must be maintained in a confidential manner at all times.

As an individual authorized to access student data, you are required to maintain this information in a confidential manner. Any unauthorized access to, modification, deletion, or disclosure of these data is a violation of this agreement and potentially a violation of state and federal laws governing the confidentiality of education data, and it could constitute a punishable act.

Unauthorized viewing, reproducing/copying, and/or distribution of any student record or information outside the intended and approved use are strictly prohibited. Users violating this agreement will lose access privileges to the data.

I certify that I have reviewed PDE's Student Data Access and Use Policy Statement. I hereby acknowledge and agree to comply with the Policy and the above requirements.

I agree

I do not agree

Signature

Date

Typed Name:

Title:

School Name: