



TENNESSEE DEPARTMENT OF  
**EDUCATION**  
FIRST TO THE TOP

**Document Approval Form**

**Date of Request for Document Review and Execution:**

November 4, 2014

**Purpose of Document:**

To execute and publish the **Data Access and Use Policy**. This is the new policy on access and use of individual student and teacher data maintained by the TDOE. It will apply to all TDOE employees and will ensure TDOE complies with all state and federal laws regarding the confidentiality of student and teacher data.

**Deadline for Document Execution:**

Immediately

**Program Approval**

By signing below, the Assistant Commissioner for the program area requesting the execution of the document certifies he/she has approved the document:

---

Assistant Commissioner Signature & Date

**Legal Approval**

By signing below, the department's legal staff certifies that the document has been reviewed and is ready for execution by the commissioner or designee:

*Christy Ballard* 11/4/14

---

Attorney Signature & Date



# TENNESSEE DEPARTMENT OF EDUCATION

FIRST TO THE TOP

<b>Approved by:</b> Kevin Huffman, Commissioner	<b>Policy Number:</b>
<b>Signature:</b> 	<b>Revised Date:</b> November 5, 2014
<b>Application:</b> All TDOE Employees	<b>Authority:</b> Tenn. Code Ann. § 49-1-201

## Data Access and Use Policy

### I. Policy Statement

The Tennessee Department of Education (TDOE) collects education records from local schools and districts as required by federal and state laws and regulations. This policy statement pertains to individual student and teacher data collected and maintained by TDOE. Individual student and teacher data are used for state and federal reporting, including the federal *Elementary and Secondary Education Act*, state assessments, state aid, state funding calculations, special education and other program participation and to improve instruction. Student demographic and performance data maintained by the TDOE is linked to a unique numerical identifier to be utilized for the purposes of satisfying federal and state reporting requirements and improving education for all students in the state. Individual student and teacher data are managed by TDOE in compliance with the following laws and their implementing regulations:

- Family Educational Rights and Privacy Act of 1974 (FERPA)
- Individuals with Disabilities Education Act (IDEA)
- National School Lunch Act
- Tennessee statutes, regulations and policies governing the confidentiality of, and access to, students' educational records and individual teacher records, including Tenn. Code Ann. §§ 10-7-504 and 49-1-606

This policy statement contains information about the procedures that will be used to ensure the confidentiality of student and teacher information and data maintained by TDOE. This policy does not expand or in any way change the allowable uses by staff of these data or the availability of student and teacher data to any other educator or member of the public.

## **II. Purpose**

To ensure the confidentiality of data maintained by the TDOE, the TDOE will not release or disclose personally identifiable student or teacher level data 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 TDOE staff and any contractors, subcontractors and their agents.

Questions from TDOE staff regarding this policy or the release of student or teacher information should be directed to the Data Quality and Integrity team as identified by the Assistant Commissioner of Data and Research. Any other individual with questions regarding student or teacher information or this policy should contact the Director of Communications.

The student data collected by TDOE are for the purpose of complying with state and federal laws and regulations, to support better decision-making, and policies to improve the performance of students and schools. TDOE data systems 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.

Information is collected on Tennessee 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). TDOE shall establish a system that maintains data in accordance with FERPA and other relevant state and federal laws and regulations.

## **III. Definitions and Background Information Related to this Policy**

The following definitions apply to 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 or teacher 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. Confidential data is not a public record. Information which allows for the identification of an individual student and that is collected by TDOE is considered personally identifiable information and may not be released without parental consent, except in very limited circumstances authorized in state and federal law.
- *Confidentiality* refers to TDOE'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, except in very limited circumstances authorized in state and federal law.
- *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* include, but are 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.

#### **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 (Student ID)

The StudentID is a seven 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 StudentID database contains a selected set of data about individual students that will allow for the assignment of a unique student identifier. The StudentID 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 StudentID. For example, upon receiving a student who has transferred into his/her LEA from another LEA within Tennessee, 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 Tennessee 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 TDOE.

##### Data Security

Security includes the technical measures put into place by the State of Tennessee to ensure that records are not lost, stolen, vandalized, illegally accessed, or otherwise rendered useless. The state will ensure 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 state and federal security policies shall be followed and regularly audited.

##### Restricted Access to Student Level Data

- **LEA and School Personnel**

The director of schools of an LEA, or his/her designee, is responsible for authorizing access to data concerning students enrolled in that LEA. An individual will be granted access to specific TDOE data systems upon receiving approval of the director of schools or his/her designee. LEAs should have on file an Acceptable Use policy form signed by the employee granted access to

TDOE data systems. LEAs will only be allowed to view their own student level district data as transferred from the LEA's source system to the TDOE data systems. LEA staff may only use the search functionality for the purpose of locating students already assigned a StudentID.

- **TDOE Staff**

Access to student level data by TDOE staff will be granted on an individual basis. Any TDOE employee or authorized agent assigned responsibilities that require student level data access must sign a data confidentiality agreement. 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 will be based on the staff member's responsibilities.

- **Other Access**

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

#### Access Exceptions

Under this Policy, no personally identifiable student information will be released without the consent of the parent or eligible student except as authorized under state and federal law including:

- (1) To school officials of the LEA in which the student is currently enrolled who have a legitimate educational interest in the information, with the approval of the director of schools or designee. School official includes contractors, consultants, volunteers, or other parties to whom an LEA or the TDOE has outsourced institutional services but are also subject to this policy;
- (2) To LEA and school personnel where a student seeks or intends to enroll;
- (3) To comply with a lawfully issued subpoena or court order;
- (4) To educational officials in connection with an audit or evaluation of a federal or state supported education program;
- (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;
- (6) To organizations conducting studies for, or on behalf of the TDOE or an LEA to develop, validate, or administer predictive tests, administer student aid programs; or improve instruction.

#### Record of Access

The Assistant Commissioner of Data and Research, 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 TDOE employee granted access as previously identified;
- (4) A party with written consent from the parent or eligible student; or
- (5) 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

TDOE 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 TDOE 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 commissioner will enforce statistical cutoff procedures using a minimum confidentiality  $n$  of 10 to ensure that student confidentiality is maintained. It is the intent of TDOE to avoid the possibility of inadvertently reporting personally identifiable information about any student.

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

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 TDOE enters into a contract with an outside entity or other state agency to perform any of the data reporting or statistical analysis, or other studies on behalf of the TDOE or an LEA, that agreement shall require that the data be protected in the same manner. TDOE will aggregate the individual student data to comply with required state and federal reporting.

### Agency Data Sharing

TDOE has inter-agency agreements to share limited amounts of data for the benefit of the children of Tennessee, as allowed by law. All sharing of student data must comply with the requirements of federal and state law and this policy.

### Parents

Upon request and in compliance with state and federal law and regulations, the Assistant Commissioner of Data and Research, 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 Assistant Commissioner of Data and Research, or his /her designee, in consultation with the General Counsel, 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 TDOE for the lawful release of student data, the commissioner, or his/her designee, will deny the request. The Assistant Commissioner of Data and Research, in consultation with the General Counsel, is also responsible for determining if personally identifiable or confidential information has been inappropriately disclosed by a TDOE employee or authorized agent in violation of this policy. Such disclosure, which may constitute a violation of law, may be subject to a disciplinary action, up to and including termination (if a TDOE employee), or permanent suspension of login privileges. If an improper disclosure is made by someone other than a TDOE employee or authorized agent, then the involved parties will not have access to any student data for at least five years. Any TDOE employee or authorized agent who has knowledge of an improper disclosure of personally identifiable or confidential student data shall report such disclosure immediately to the Assistant Commissioner of Data and Research and the General Counsel. Failure to report a disclosure may result in disciplinary action.

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

LEAs or other primary sources of the data that are located at TDOE are the originators and owners of those data. The Chief Information Officer functions as the custodian of the data in the TDOE. The custodian is charged with implementing and maintaining security controls for data pursuant to this policy. The policy ensures that all data are securely maintained with safeguards on all personally identifiable or confidential information.