



SECTION III: STUDENT POLICY 3150

Student Data Access and Use Policy

I. Introduction/Background

This policy statement pertains to individual student data collected and maintained by Insight School of Oklahoma (ISOK) using Student Information Management Systems (SIMS). Individual student data are used for the purpose of collecting data needed for state and federal reporting, state assessments, state aid, special education and program participation as well as to satisfy other data requests from the State Department of Education (SDE), the state legislature, and other authorized entities.

Collecting Student Data

ISOK will collect the following student data. All student data will be collected and maintained in the student's cumulative record:

- Student Name
- Birth Certificate US or Country of Origin/student's age, per state guidelines
- Proof of Residence, per state guidelines
- Immunization record, per state guidelines
- Free and Reduce Lunch Status, per state guidelines
- School behavior record, including suspension and expulsion records (as appropriate)
- Special education program information (as appropriate), including:
 - an individualized education program;
 - a Section 504 accommodation plan; or
 - an English learner plan.

ISOK will collect the following **optional data**, based on individual student need:

- School Transcripts
- Promotion, Grade Placement, and Retention History
- Attendance history
- High School course credit history
- Report Cards
- Academic testing results such as OCCT, ACT, Dibels, and interim assessments
- Court Documents signed or stamped by the Judge, Magistrate, or deputy clerk
- Court Orders
- Proof of legal guardianship, per state guidelines
- Department of Child Services Documentation
- English Language Learning needs
- Medical and social developmental history, as necessary to ensure educational access and programming

- Evaluation reports, such as cognitive and achievement data, as necessary to ensure educational access and programming
- Vision and Hearing Screenings

Individual student data are managed by ISOK 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), and Oklahoma 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 ISOK. 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 SIMS is intended to support better decision-making and policies for improving the performance of students and schools. ISOK intends that SIMS will ultimately reduce the reporting burden, help to facilitate the entry of students into ISOK or transfer to a new school and ensure that timely, high quality data are available to authorized users.

II. Definitions of Background Information Related to this Policy.

ISOK 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 Oklahoma statutes. 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 ISOK 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 ISOK'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, 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 identify 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;
- ISOK manages student information under its control throughout its life cycle, from original submission to appropriate destruction;
- ISOK 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 school level;
- ISOK is responsible for reviewing and updating policies and regulations covering confidential student information and ensuring that its activities comply with state and federal law;
- ISOK 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, and restricted access.

Assignment of a Unique Identifier (TV Student ID)

The TV Student ID is a 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 TV Student ID database contains a selected set of data about individual students that will allow for the assignment of a unique student identifier. The TV Student ID 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 SCHOOL identification number of the student. After being checked for duplicates, the number is made permanent.

Data Security

Security includes the technical measures put into place by ISOK 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 or 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 Oklahoma and federal security policies shall be followed and regularly audited.

Restricted Access to Student Level Data

School Personnel

The chief school administrator or his/her designee is responsible for authorizing access to data concerning students enrolled at ISOK. 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.

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.

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 ISOK 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.

ISOK will aggregate the individual student data to comply with required state and federal reporting.

Agency Data Sharing

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

Researchers

Aggregate Information

ISOK may respond 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.

Section 99.31 (a)(6) of the FERPA regulations permits information about individual students to be released without parental permission to researchers conducting studies for or on behalf of the SDE 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 SDE must have authorized the study and it must be conducted for or on behalf of the SDE. 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 SDE.

Parents

Upon request, and as specified under Section 99.10(a)(2) of the FERPA regulations, the chief school administrator 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 chief school administrator 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 ISOK for the lawful release of student data, then the chief school administrator or his/her designee will deny the request.

The chief school administrator is also responsible for determining if personally identifiable or confidential information has been inappropriately disclosed by an ISOK 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 an ISOK employee), or suspension of login privileges. If an improper disclosure is made by someone other than an ISOK employee or authorized agent, then the involved parties will not have access to any student data for five years.

VII. Ownership of the Data

Sources of the data that are located at ISOK are the originators and owners of those data. The chief school administrator functions as the custodian of the data in ISOK. In order to protect the data in its custody, the ISOK Board of Education has established this policy that is implemented by the chief school administrator. 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 Insight School of Oklahoma Student 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 ISOK'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

Printed name: _____ Title: _____