Insight School of Oklahoma Student Data Privacy Policy

Insight School of Oklahoma (ISOK) collects the necessary student data and stores this data in the students' cumulative record, to ensure the students' unique educational needs and appropriate programming can be addressed. Insight School of Oklahoma will comply with the Student Data Accessibility, Transparency and Accountability Act of 2013 (70 O.S. § 3-168) concerning the privacy of student data maintained by the school.

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

Sharing Student Data

The Student Data Accessibility, Transparency and Accountability Act of 2013 (70 O.S. § 3-168) states that the education entity may not share student data without a data authorization. ISOK may not share a student's personally identifiable student data if the personally identifiable student data is not shared in accordance with the Family Education Rights and Privacy Act.

The Family Educational Rights and Privacy Act (FERPA) affords parents and students who are 18 years of age or older ("eligible students") certain rights with respect to the student's education records that are maintained by the local school district. These rights are:

1. **The right to inspect and review the student's education records within 45 days after the day the student's school receives a request for access.**

   Parents or eligible students should submit a written request to the school principal (or the official designated by the school for purposes of processing FERPA requests) that identifies the records they wish to inspect. The school official will make arrangements for access and notify the parent or eligible student of the time and place where the records may be inspected.

2. **The right to request the amendment of the student's education records that the parent or eligible student believes are inaccurate, misleading, or otherwise in violation of the student's privacy rights under FERPA.**

   Parents or eligible students who wish to ask the student's school to amend a record should write the school principal (or other official designated by the school), clearly identify the part of the record they want changed, and specify why it should be changed. If the school decides not to amend the record as requested by the parent or eligible student, the school will notify the parent or eligible student of the decision and of their right to a hearing regarding the request for amendment. Additional information regarding the hearing procedures will be provided to the parent or eligible student when notified of the right to a hearing.

3. **The right to provide written consent before the school discloses personally identifiable information (PII) from the student's education records, except to the extent that FERPA authorizes disclosure without consent.**

   One exception, which permits disclosure without consent, is disclosure to school officials with legitimate educational interests. A school official is a person employed by the school as an administrator, supervisor, instructor, or support staff member (including health or medical staff and law enforcement unit personnel) or a person serving on the school board. A school official also may include a volunteer or contractor outside of the school who performs an institutional service of function for which the school would otherwise use its own employees and who is under the direct control of the school with respect to the use and maintenance of PII from education records, such as an attorney, auditor, medical consultant, or therapist; a parent or student volunteering to serve on an official committee, such as a disciplinary or grievance committee; or a parent, student, or other volunteer assisting another school official in

performing his or her tasks. A school official has a legitimate educational interest if the official needs to review an education record in order to fulfill his or her professional responsibility.

Upon request, the student's school may disclose education records without consent to officials of another school district in which a student seeks or intends to enroll, or is already enrolled if the disclosure is for purposes of the student's enrollment or transfer. FERPA requires a school district to make a reasonable attempt to notify the parent or student of the records request unless it states in its annual notification that it intends to forward records on request.

FERPA permits the disclosure of PII from students' education records, without consent of the parent or eligible student, if the disclosure meets certain conditions found in §99.31 of the FERPA regulations. Except for disclosures to school officials, disclosures related to some judicial orders or lawfully issued subpoenas, disclosures of directory information, and disclosures to the parent or eligible student, §99.32 of the FERPA regulations requires the school to record the disclosure. Parents and eligible students have a right to inspect and review the record of disclosures. A school may disclose PII from the education records of a student without obtaining prior written consent of the parents or the eligible student in the following circumstances:

- To other school officials, including teachers, within the educational agency or institution whom the school has determined to have legitimate educational interests. This includes contractors, consultants, volunteers, or other parties to whom the school has outsourced institutional services or functions, provided that the conditions listed in §99.31(a)(1)(i)(B)(1) - (a)(1)(i)(B)(2) are met. (§99.31(a)(1))

- To officials of another school, school system, or institution of postsecondary education where the student seeks or intends to enroll, or where the student is already enrolled if the disclosure is for purposes related to the student's enrollment or transfer, subject to the requirements of §99.34. (§99.31(a)(2))

- To authorized representatives of the U. S. Comptroller General, the U. S. Attorney General, the U.S. Secretary of Education, or State and local educational authorities, such as the State educational agency in the parent or eligible student's State (SEA). Disclosures under this provision may be made, subject to the requirements of §99.35, 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. These entities may make further disclosures of PII to outside entities that are designated by them as their authorized representatives to conduct any audit, evaluation, or enforcement or compliance activity on their behalf. (§§99.31(a)(3) and 99.35)

- In connection with financial aid for which the student has applied or which the student has received, if the information is necessary to determine eligibility for the aid, determine the amount of the aid, determine the conditions of the aid, or enforce the terms and conditions of the aid. (§99.31(a)(4))

- To State and local officials or authorities to whom information is specifically allowed to be reported or disclosed by a State statute that concerns the juvenile justice system and the system's ability to effectively serve, prior to adjudication, the student whose records were released, subject to §99.38. (§99.31(a)(5))

- To organizations conducting studies for, or on behalf of, the school, in order to: (a) develop, validate, or administer predictive tests; (b) administer student aid programs; or (c) improve instruction. (§99.31(a)(6))

    - To accrediting organizations to carry out their accrediting functions. (§99.31(a)(7))

    - To parents of an eligible student if the student is a dependent for IRS tax purposes. (§99.31(a)(8))

    - To comply with a judicial order or lawfully issued subpoena. (§99.31(a)(9))

    - To appropriate officials in connection with a health or safety emergency, subject to §99.36. (§99.31(a)(10)

    - Information the school has designated as "directory information" under §99.37. (§99.31(a)(11))

4. **The right to file a complaint with the U.S. Department of Education concerning alleged failures by the ISOK to comply with the requirements of FERPA.**

    The name and address of the Office that administers FERPA are:
    Family Policy Compliance Office
    U.S. Department of Education
    400 Maryland Avenue, SW
    Washington, DC 20202

Collection, Use, and Sharing Student Data

The collection, use, and sharing of student data has both benefits and risks. Parents and students should learn about these benefits and risks and make choices regarding student data accordingly.

Student data is collected by ISOK during the enrollment process and through the parent portal. All data collected during this process is maintained in a digital format.

Storage of online data is securely maintained and data backups occur daily. Data is backed up to a separate, disk-based storage system in a secure, geographically segregated data center for optimal protection.

This data is considered to be critical data and is capable of surviving a disaster (fire, water damage, etc.). The data is stored in a world class, biometrically secured level 3 data center.

K12 also employs a data replication strategy and architecture. In addition to the daily data backups, data is continually replicated to our geographically segregated contingency data center for the purposes of disaster recovery. Our data replication strategy protects against data loss should our primary data center experience a catastrophic event requiring K12 to run system operations from our contingency data center.