

IDAE **Student Privacy Policy**
(See BCBK, ICA, ICAA, II, and JR et seq.)

IDAE

The superintendent, the board and staff shall protect the right of privacy of students and their families in connection with any surveys or physical examinations conducted, assisted, or authorized by the board or administration. The district shall annually provide parents notice of their rights under the Protection of Pupil Rights Amendment and the Student Data Privacy Act, at the beginning of each school year, and at any other time the school district policies in the area are substantially changed.

Student Data Restrictions

Any student data submitted to or maintained in a statewide longitudinal student data system shall only be disclosed in accordance with the Student Data Privacy Act. Disclosure of all other student data or student record information maintained is governed by the Family Educational Rights and Privacy Act (“FERPA”).

Annual written notice presented to parents and legal guardians of district students shall: 1) require parent or guardian’s signature; and 2) shall state student data submitted to or maintained in a statewide longitudinal data system only be disclosed as follows.

Student data may be disclosed to:

- The authorized personnel of an educational agency or the state board of regents who require disclosures to perform assigned duties; and
- The student and the parent or legal guardian of the student, provided the data pertains solely to the student.

Student data may be disclosed to authorized personnel of any state agency, or to a service provider of a state agency, educational agency, or school

performing instruction, assessment, or longitudinal reporting, provided a data-sharing agreement between the educational agency and other state agency or service provider provides the following:

- purpose, scope and duration of the data-sharing agreement;
- recipient of student data use such information solely for the purposes specified in agreement;
- recipient shall comply with data access, use, and security restrictions specifically described in agreement; and
- student data shall be destroyed when no longer necessary for purposes of the data-sharing agreement or upon expiration of the agreement, whichever occurs first.

*A service provider engaged to perform a function of instruction may be allowed to retain student transcripts as required by applicable laws and rules and regulations. Destruction shall comply with the NISTSP800-88 standards of data destruction.

Unless an adult student or parent or guardian of a minor student provides written consent to disclose personally identifiable student data, student data may only be disclosed to a governmental entity not specified above or any public or private audit and evaluation or research organization if the data is aggregate data. "Aggregate data" means data collected or reported at the group, cohort, or institutional level and which contains no personally identifiable student data.

The district may disclose:

- Student directory information when necessary and the student's parent or legal guardian has consented in writing;
- directory information to an enhancement vendor providing photography services, class ring services, yearbook publishing services, memorabilia services, or similar services;
- any information requiring disclosure pursuant to state statutes;
- student data pursuant to any lawful subpoena or court order directing such disclosure; and
- student data to a public or private postsecondary educational institution for purposes of application or admission of a student to such postsecondary educational institution with the student's written consent.

Student Data Security Breach

If there is a security breach or unauthorized disclosure of student data or personally identifiable information of any student submitted to or maintained on a statewide student longitudinal data system, each affected student or the parent or legal guardian of the student, if a minor, shall be immediately notified, and an investigation into the causes and consequences of the breach or unauthorized disclosure will be conducted.

Biometric Data

The district shall not collect biometric data from a student or use any device or mechanism to assess a student's physiological or emotional state, unless the adult student or the parent or legal guardian of the minor student consents in writing. "Biometric data" includes measurable biological or behavioral characteristics that can be used for automated recognition of an

individual, such as fingerprints, retina and iris patterns, voiceprints, DNA sequence, facial characteristics, and handwriting.

Nothing in this policy shall prohibit the collection of audio voice recordings, facial expression information, and student handwriting for:

- provision of counseling or psychological services,
- conducting student threat assessments,
- completing student disciplinary investigations or hearings, or
- conducting child abuse investigations.

Select Student Surveys

No test, questionnaire, survey, or examination containing any questions about a student's or the student's parents' or guardians' personal beliefs or practices on issues such as sex, family life, morality, or religion shall be administered to any student unless:

- the parent or guardian is notified in writing; and
- the parent or guardian of the student gives written permission for the student to participate.

Nothing shall prohibit school counselors from providing counseling services, including the administration of tests and forms as part of student counseling services. Any information obtained through such tests or counseling services shall not be stored on any personal mobile electronic device which is not owned by the school district. Storage of such information on personal laptops, tablets, phones, flash drives, external hard drives, or virtual servers not owned by the district is prohibited.

Students may be questioned:

- in the provision of psychological services,
- conducting of student threat assessments,
- completing student disciplinary investigations or hearings, or
- conducting child abuse investigations.

Collection of such information in these limited circumstances is permitted without prior written consent of the parent, guardian, or adult student.

Approved: August 11, 2014

Annual Notice of Authorized Student Data Disclosures

In accordance with the Student Data Privacy Act and board policy IDAE, student data submitted to or maintained in a statewide longitudinal data system may only be disclosed as follows. Such data may be disclosed to:

- The authorized personnel of an educational agency or the state board of regents who require disclosures to perform assigned duties; and
- The student and the parent or legal guardian of the student, provided the data pertains solely to the student.

Student data may be disclosed to authorized personnel of any state agency, or to a service provider of a state agency, educational agency, or school performing instruction, assessment, or longitudinal reporting, provided a data-sharing agreement between the educational agency and other state agency or service provider provides the following:

- purpose, scope and duration of the data-sharing agreement;
- recipient of student data use such information solely for the purposes specified in agreement;
- recipient shall comply with data access, use, and security restrictions specifically described in agreement; and
- student data shall be destroyed when no longer necessary for purposes of the data-sharing agreement or upon expiration of the agreement, whichever occurs first.

*A service provider engaged to perform a function of instruction may be allowed to retain student transcripts as required by applicable laws and rules and regulations.

Unless an adult student or parent or guardian of a minor student provides written consent to disclose personally identifiable student data, student data may only be disclosed to a governmental entity not specified above or any public or private audit and evaluation or research organization if the data is aggregate data. "Aggregate data" means data collected or reported at the group, cohort, or institutional level and which contains no personally identifiable student data.

The district may disclose:

- Student directory information when necessary and the student's parent or legal guardian has consented in writing;
- directory information to an enhancement vendor providing photography services, class ring services, yearbook publishing services, memorabilia services, or similar services;
- any information requiring disclosure pursuant to state statutes;
- student data pursuant to any lawful subpoena or court order directing such disclosure; and
- student data to a public or private postsecondary educational institution for purposes of application or admission of a student to such postsecondary educational institution with the student's written consent.

As the parent or legal guardian of [name of student(s)], I acknowledge that I have been provided with notice of authorized student data disclosures under the Student Data Privacy Act.

Parent Signature

Date