FERPA & MANAGEMENT OF STUDENT RECORDS POLICY – STUDENT DATA PRIVACY & SECURITY

~~Drafted by the Data Management Council (DMC) and adopted by the Idaho State Board of Education - Effective August 14, 2014~~

The efficient collection, analysis, and storage of student information is essential to improve the education of our students. As the use of student data has increased and technology has advanced, the need to exercise care in the handling of confidential student information has intensified. The privacy of students and the use of confidential student information is protected by federal and state laws, including the Family Educational Rights and Privacy Act (FERPA) and the Idaho Student Data Accessibility, Transparency and Accountability Act of 2014 (Idaho Data Accountability Act, Idaho Code §33-133).

Student information is compiled and used to evaluate and improve Idaho's educational system and improve transitions from high school to postsecondary education or the workforce. The Data Management Council (DMC) was established by the Idaho State Board of Education to make recommendations on the proper collection, protection, storage, and use of confidential student information stored within the Statewide Longitudinal Data System (SLDS). The DMC includes representatives from K-12, higher education institutions and the Department of Labor.

This policy is required by the Idaho Data Accountability Act. In order to ensure the proper protection of confidential student information, **this** ~~each school~~ district **is required to** ~~shall~~ adopt, implement, and electronically post this policy. It is intended to provide guidance regarding the collection, access, security, and use of education data to protect student privacy. This policy is consistent with all FERPA regulations and with DMC's policies regarding the access, security, and use of data maintained within the SLDS. Violation of the Idaho Data Accountability Act may result in civil penalties as set forth in Idaho Code §33-133.

DEFINED TERMS

Administrative Security consists of policies, procedures, areas of responsibility, user access controls, and personnel controls including security policies, training, and audits, technical training, supervision, separation of duties, rotation of duties, recruiting and termination procedures, user access control, background checks, performance evaluations, and disaster recovery, contingency, and emergency plans. These measures ensure that authorized users know and understand how to properly use the system in order to maintain security of data.

Aggregate Data is collected or reported at a group, cohort, or institutional level and does not contain PII (Personally Identifiable Information).

Data Breach is the unauthorized acquisition of personally identifiable information (PII) as defined herein.

Logical Security consists of software safeguards for an organization's systems, including user identification and password access, authenticating, access rights and authority levels. These measures ensure that only authorized users are able to perform actions or access information in a network or at a workstation

Personally Identifiable Information (PII) includes the following: a student's name; the name of a student's family; the student's address; the students' social security number; a student education unique identification number or biometric record; or other indirect identifiers such as a student's date of birth, place of birth, or mother's maiden name, and other information that alone or in combination is linked or linkable to a specific student that would allow a reasonable person in the school community who does not have personal knowledge of the relevant circumstances to identify the student.

Physical Security describes security measures designed to deny unauthorized access to facilities or equipment.

Student Data means data collected at the student level and included in a student's educational records.

Student Educational Record means all information directly related to a student and recorded and kept in the data system, as that term is defined in this policy, and may include information considered to be personally identifiable. A student educational record shall not include: (1) juvenile delinquency records and criminal records unless required by law; (2) medical and health records; (3) student social security number; (4) student biometric information; (5) gun ownership records; (6) sexual orientation; (7) religious affiliation; (8) except for special needs and exceptional students, any data collected pursuant to a statewide assessment via affective computing, including analysis of facial expressions, EEG brain wave patterns, skin conductance, galvanic skin response, heart rate variability, pulse, blood volume, posture and eye tracking, any data that measures psychological resources, mind sets, effortful control, attributes, dispositions, social skills, attitudes or intrapersonal resources.

Student education unique identification number means the unique student identifier assigned by the state to each student that shall not be or include the social security number of a student in whole or in part.

Unauthorized Data Disclosure is the intentional or unintentional release of PII to an unauthorized person or untrusted environment.

COLLECTION

The school district shall follow applicable state and federal laws related to student privacy in the collection of student data.

ACCESS

Unless prohibited by law or court order, **the** ~~school~~ district shall provide parents, legal guardians, or eligible students, as applicable, the ability to review their child's educational records.

The Superintendent, administrator, or designee, is responsible for granting, removing, and reviewing user access to student data. An annual review of existing access shall be performed.

Access to PII maintained by the ~~school~~ district shall be restricted to the following: (1) the authorized staff of the school district who require access to perform their assigned duties; (2) authorized employees of the State Board of Education (SBE) and the State Department of Education (SDE) who require access to perform their assigned duties; and (3) vendors of the SBE, SDE or IDLA who require access to perform their assigned duties; (4) students and/or their parents or legal guardians; (5) the authorized staff of other state agencies in Idaho as required by law and/or defined by interagency data-sharing agreements.

SECURITY

The ~~School~~ districts shall have in place Administrative Security, Physical Security, and Logical Security controls to protect from a Data Breach or Unauthorized Data Disclosure.

The ~~School~~ district shall immediately notify the Executive Director of the Idaho State Board of Education and the State Superintendent of Public Education in the case of a confirmed Data Breach or confirmed Unauthorized Data Disclosure.

The ~~School~~ district shall notify in a timely manner affected individuals, students, and families if there is a confirmed Data Breach or confirmed Unauthorized Data Disclosure.

USE

Publicly released reports shall not include PII and shall use Aggregate Data in such a manner that re-identification of individual students is not possible.

The ~~School~~ district contracts with outside vendors involving student data, which govern databases, online services, assessments, special education, or instructional supports, shall include the following provisions that are intended to safeguard student privacy and the security of the data:

- Requirement that the vendor agree to comply with all applicable state and federal law;
- Requirement that the vendor have in place Administrative Security, Physical Security, and Logical Security controls to protect from a Data Breach or Unauthorized Data Disclosure;
- Requirement that the vendor restrict access to PII to the authorized staff of the vendor who require such access to perform their assigned duties;
- Prohibition against the vendor's secondary use of PII including sales, marketing, or advertising;
- Requirement for data destruction and an associated timeframe; and
- Penalties for non-compliance with the above provisions.

The ~~School~~ district shall clearly define what data is determined to be directory information as stated in the FERPA Notice published annually in the local newspaper and on the district website.

If **the** ~~a school~~ district chooses to publish directory information that includes PII, parents will be notified annually in writing, via the FERPA Notice published annually in the local newspaper and on the district website, and also given an opportunity to opt out of the directory. If a parent does not opt out, the release of the information as part of the directory is not a Data Breach or Unauthorized Data Disclosure.

♦ ♦ ♦ ♦ ♦ ♦ ♦

LEGAL REFERENCE:

Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. §1232g)

Electronic Code of Federal Regulations pertaining to FERPA: 34 CFR Part 99

U.S. Department of Education, Student Privacy Policy Office

Idaho Student Data Accessibility, Transparency, and Accountability Act of 2014, Idaho Code Title 33, Section 33-133

ADOPTED: August 14, 2014/September 16, 2014

Revised: July 19, 2016 Reviewed: March 16, 2021