STUDENT DATA PRIVACY AND SECURITY

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).

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. In order to ensure the proper protection of confidential student information, the Bonneville Joint School District Board of Trustees requires that student information shall be safeguarded and privacy shall be protected with regard to collection, access, security, and use of education data maintained within the State Longitudinal Data Systems (SLDS). Therefore the Board directs the Superintendent/designee to follow applicable state and federal law to ensure proper protection of confidential student information in the collection or such data.

Guidelines

Access

1. Unless prohibited by law or court order and pursuant to policy #3600 ***Student Records,*** parents, legal guardians, or eligible students, as applicable, shall be provided the ability to review their child's or their own educational records.

2. The Superintendent or designee is responsible for granting, removing, and reviewing user access to student data.

3. An annual review of existing access shall be performed.

4. Access to PII student data maintained by the District shall be restricted to:

    a. Authorized staff of the District who require access in order to perform their assigned duties;

    b. Authorized employees of the State Board of Education and the State Department of Education who require access in order to perform their assigned duties; and

c. Vendors who require access to perform their assigned duties.

Security

The District shall:

1. Have in place Administrative Security, Physical Security, and Logical Security controls to protect from a Data Breach or Unauthorized Data Disclosure;

2. In the case of a confirmed Data Breach or a confirmed Unauthorized Data Disclosure:

   a. Immediately notify the Executive Director of the Idaho State Board of Education and the State Superintendent of Public Instruction; and

   b. Notify in a timely manner affected individuals, students, and families.

Use

1. 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.

2. District contracts with outside vendors which govern databases, online services, assessments, special education, or instructional supports, shall include the following provisions which are intended to safeguard student privacy and security of data.

   a. Requirement that the vendor agree to comply with all applicable state and federal law.

   b. 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.

   c. Requirement that the vendor restrict access to PII to the authorized staff of the vendor who require such access to perform their assigned duties;

   d. Prohibition against the vendor’s secondary use of PII including sales, marketing or advertising;

   e. Requirement for data destruction and an associated timeframe; and

   f. Penalties for non-compliance with the above provisions.

Directory Information

1. The District shall clearly define what data is determined to be directory information.

2. If the District chooses to define and publish directory information that includes PII; parents, legal guardians, and eligible students shall be notified annually in writing using exhibit #3600E *Student Records-Notification of Parents and Students of Rights* and given an opportunity to opt out of the directory using the *Student Directory Information Opt-Out* Form #3600F.

3. If a parent, legal guardian, or eligible student does not opt out, the release of the information as part of the directory is not a Data Breach or Unauthorized Data Disclosure.

Violation

Violation of the Idaho Data Accountability act may result in civil penalties.

DEFINITIONS

Administrative Security: consists of policies, procedures, 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 the group, cohort, or institutional level and does not contain Personally Identifiable Information (PII).

Data Breach: is the unauthorized acquisition of PII.

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 a workstation.

Personally Identifiable Information (PII): includes: a student's name; the name of a student's parent or family members; 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 that are designed to deny unauthorized access to facilities or equipment.

State Longitudinal Data Systems (SLDS): is the state's elementary, secondary, and postsecondary longitudinal data systems

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

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

Adopted 10-08-2014 Reviewed Revised

Cross Reference: Student Records #3600
Student Records Procedures #3600P
Records of Missing Children #3605

Legal Reference: Idaho Code § 33-133 Idaho Student Data Accessibility, Transparency, and Accountability Act of 2014
Idaho Code § 33-209 Transfer of Student Records -- Duties
20 U.S.C. § 1232g and 34 C.F.R. 99 Family Education Rights and Privacy Act