

Policy 1020-10

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.

This policy is required by the Idaho Data Accountability Act. In order to ensure the proper protection of confidential student information, the District shall adopt, implement and electronically post this policy to its website. 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 the 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.

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 a group, cohort, or institutional level and does not contain 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 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.
- **Unauthorized Data Disclosure:** is the intentional or unintentional release of PII to an unauthorized person or untrusted environment.

Collection

The 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 District shall provide parents, legal guardians, or eligible students, as applicable, the ability to review their child's educational records.

The Superintendent 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 District shall be restricted to:

1. The authorized staff of the District who require access to perform their assigned duties; and
2. Authorized employees of the State Board of Education and the State Department of Education who require access to perform their assigned duties; and
3. Vendors who require access to perform their assigned duties.

Security

The District shall have in place Administrative Security, Physical Security, and Logical Security controls to protect from a Data Breach or Unauthorized Data Disclosure. The District shall immediately notify the Executive Director of the Idaho State Board of Education and the State Superintendent of Public Instruction in the case of a confirmed Data Breach or confirmed Unauthorized Data Disclosure. The District shall also 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.

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

1. Requirement that the vendor agree to comply with all applicable State and federal law;
2. 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;
3. Requirement that the vendor restrict access to PII to the authorized staff of the vendor who require such access to perform their assigned duties;
4. Prohibition against the vendor's secondary use of PII including sales, marketing or advertising;
5. Requirement for data destruction and an associated timeframe; and
6. Penalties for non-compliance with the above provisions.

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

If the District chooses to publish directory information which includes PII, parents must be notified annually in writing and given an opportunity to opt out of the directory within a specified period of time. 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.