PAYETTE SCHOOL DISTRICT POLICY

416 STUDENT DATA PRIVACY AND SECURITY POLICY (Adopted 10-13-14)

The efficient collection, analysis, and storage of student information are 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. This policy ensures the proper protection of confidential student information.

Defined Terms

Administrative Security consists of policies, procedures, and personnel control to include technical training, supervision, user access control, background checks, performance evaluations, disaster recovery, contingency, and emergency plans.

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 including user identification and password access, access rights, and authority levels.

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 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, schools shall provide parents, legal guardians, or eligible students the ability to review their child's educational records.
  The superintendent, building administrator, or designee is responsible for granting, removing, and reviewing user access to student data.
- Access to PII maintained by the school district shall be restricted to: (1) the authorized staff of the school 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 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 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.
- 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:
  - 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.

- 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. 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.