STUDENT DATA PRIVACY AND SECURITY POLICY #8000

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).

This policy is consistent with the DMC's policies regarding the access, security and use of data maintained within the SLDS.[1] Violation of the Idaho Data Accountability Act may result in civil penalties.[2]

Defined Terms

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.

School means Rolling Hills Public Charter School.

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

---

[1] Data Management Council Policies and Procedures
[2] Idaho Code Title 33, Section 133

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

Collection

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

The administrator 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 shall be restricted to:

> (1) the authorized staff of the School 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 School shall have in place Administrative Security, Physical Security, and Logical Security controls to protect from a Data Breach or Unauthorized Data Disclosure.

The School 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 School 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.

School 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.

Upon signing a new School contract, or at least annually for standing contracts, School contracts will be reviewed for compliance with these provisions, or vendors shall be required to provide evidence of compliance with these requirements.

Directory Information

The School may use student name, grade, classroom, phone number, parent name, physical (home) address, and email address as Directory Information.

Parents shall be notified annually if the School intends to publish directory information and given the 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.

Policy History

Adopted: 8-13-2014