Student Data Privacy and Security Policy

The efficient collection, analysis, and storage of student information is essential to improving the quality of education provided to our students. As the use of student data has increased and technology has advanced, the need to exercise care in 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 Rhode Island Educational Records Bill of Rights.

Student information is compiled and used to evaluate and improve our educational system and improve transitions from high school to postsecondary education or the workforce. This policy has been developed to ensure the proper protection of confidential student information. It is intended to provide guidance regarding the collection, access, security and use of educational data to protect student privacy.

Defined Terms

Aggregate Data is collected or reported at a 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 from a device.

Personally Identifiable Information (PII) includes: a student's name; the name of a student's family; the student's address; a student education unique identification; 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.

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

- All state and federal laws related to student privacy in the collection of student data must be followed.

Access

- Unless prohibited by law or court order, the district/schools 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.
- Access to student data maintained by the district/schools 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 Rhode Island Department of Education (RIDE) who require access to perform their assigned duties; and (3) vendors who require access to perform their assigned duties.

Security

- Physical Security and Logical Security shall be in place to protect from a Data Breach or Unauthorized Data Disclosure.
- Proper notification to individuals, students, families shall be made if there is a Data Breach or Unauthorized Data Disclosure.

Use

- Publicly released reports shall not include PII and shall use summarized student data in such a manner that re-identification of individual students is not possible.
- District/School contracts with outside vendors involving student data, including those which govern databases, online services, assessment, special education or instructional supports, shall include the following provisions to safeguard student privacy:
    - Private vendors shall be permitted to use aggregate student data only, unless the vendor has received written permission from the parent, legal guardian, or eligible student, as applicable, to use PII, if use is within one of the exceptions set forth in FERPA.
    - If one of the exceptions set forth under FERPA is applicable, the school district shall enter an agreement which complies with FERPA and requires the outside party to:
        - safeguard privacy and security of the data
        - restrict access to the data
        - prohibit the secondary use of data including sales, marketing or advertising
        - provide for data destruction and an associated time frame and
        - include penalties for non-compliance.
    - Vendors must agree to be able to demonstrate compliance with the Child Online Privacy and Protection Act (COPPA) by either signing on to the Student Privacy Pledge or an equivalent response to inquiry.

- If the district/school chooses to define and publish directory information which includes PII, parents must be notified annually and given an opportunity to opt out of the directory.

Resources

- FERPA: http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html
- Rhode Island Educational Records Bill of Rights: http://webserver.rilin.state.ri.us/Statutes/title16/16-71/16-71-3.htm
- COPPA: http://www.coppa.org/
- Student Privacy Pledge: http://studentprivacypledge.org/

Policy Adopted 6/4/2015