1   Meridian Technical Charter High School
2
3   Student Data Privacy and Security
4   Series 500
5
6   Policy Title: <u>Student Data Privacy and Security</u>   Code No. <u>504.61</u>
7
8   **Defined Terms**
9   **Administrative Security** consists of policies, procedures, and personnel controls including security
10   policies, training, and audits, technical training, supervision, separation of duties, rotation of duties,
11   recruiting and termination procedures, user access control, background checks, performance
12   evaluations, and disaster recovery, contingency, and emergency plans. These measures ensure that
13   authorized users know and understand how to properly use the system in order to maintain security of
14   data.
15   **Aggregate Data** is collected or reported at a group, cohort or institutional level and does not contain PII.
16   **Data Breach** is the unauthorized acquisition of PII.
17   **Logical Security** consists of software safeguards for an organization's systems, including user
18   identification and password access, authenticating, access rights and authority levels. These measures
19   ensure that only authorized users are able to perform actions or access information in a network or a
20   workstation.
21   **Personally Identifiable Information (PII)** includes: a student's name; the name of a student's family; the
22   student's address; the students' social security number; a student education unique identification
23   number or biometric record; or other indirect identifiers such as a student's date of birth, place of birth
24   or mother's maiden name; and other information that alone or in combination is linked or linkable to a
25   specific student that would allow a reasonable person in the school community who does not have
26   personal knowledge of the relevant circumstances, to identify the student.
27   **Physical Security** describes security measures designed to deny unauthorized access to facilities or
28   equipment.
29   **Student Data** means data collected at the student level and included in a student's educational records.
30   **Unauthorized Data Disclosure** is the intentional or unintentional release of PII to an unauthorized
31   person or untrusted environment.
32
33   **Collection**
34   • School districts and public charter schools shall follow applicable state and federal laws related
35   to student privacy in the collection of student data.
36
37   **Access**
38   • Unless prohibited by law or court order, school districts and public charter schools shall provide
39   parents, legal guardians, or eligible students, as applicable, the ability to review their child's
40   educational records.
41   • The Superintendent, administrator, or designee, is responsible for granting, removing, and
42   reviewing user access to student data. An annual review of existing access shall be performed.
43   • Access to PII maintained by the school district or public charter school shall be restricted to: (1)
44   the authorized staff of the school district or public charter school who require access to perform
45   their assigned duties; and (2) authorized employees of the State Board of Education and the
46   State Department of Education who require access to perform their assigned duties; and (3)
47   vendors who require access to perform their assigned duties.

48
49 **Security**
- School districts and public charter schools shall have in place Administrative Security, Physical Security, and Logical Security controls to protect from a Data Breach or Unauthorized Data Disclosure.
- School districts and public charter schools 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.
- School districts and public charter schools shall notify in a timely manner affected individuals, students, and families if there is a confirmed Data Breach or confirmed Unauthorized Data Disclosure.

59 **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 district or public charter 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:
  - 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.
- School districts and public charter schools shall clearly define what data is determined to be directory information.
- If a school district or public charter school 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.

82
83
84 Date of Revision   Legal Reference: Code of Idaho
85   3/18/2019   Idaho Code 33, Section 133