MURRAY CITY SCHOOL DISTRICT

NUMBER:	ADM230
EFFECTIVE:	8/10/2017
REVISION:	
PAGES:	3

Statement of.....

Policy and Responsibility

SUBJECT: DATA PRIVACY AND SECURITY POLICY

The efficient collection, analysis, and storage of student and employee information is essential to improve the education of our students and the smooth operation of the district. As the use of data has increased and technology has advanced, the need to exercise care in the handling of confidential information has intensified. The privacy of students and employees and the use of confidential information is protected by federal and state laws, including the Family Educational Rights and Privacy Act (FERPA).

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 personally identifiable information (PII).

Data Breach is the unauthorized acquisition of PII.

Employee Data means data collected and included in an employee's employment records.

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/employee's name; the name

of a student/employee's family; the a student/employee's address; the a student/employee's social security number; a student/employee's unique identification number or biometric record; or other indirect identifiers such as a 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/employee 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/employee privacy in the collection of 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, administrator, or designee, is responsible for granting, removing, and reviewing user access to student/employee 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 school district or public charter 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 contracted/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 notify in a timely manner affected individuals, students, employees, 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 or employees is not possible.

- If the 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:
    - 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.
- The district shall clearly define what data is determined to be directory information.
- If the district chooses to publish student 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.