Responsible Office: Office of Information Technology (IT)

BOARD POLICY 7205

INFORMATION TECHNOLOGY – DATA ACCESS POLICY

PURPOSE

The Board of Trustees (Board) of the Washoe County School District (District) is committed to ensuring the security of District computer systems, related technology, and electronic information. This Board Policy shall clarify the District's data access levels and responsibilities, delineate appropriate uses for all users of the District's computer systems, and ensure compliance with relevant state and federal law. The Board considers the security and confidentiality of student and employee records a matter of concern, and each individual who has access to confidential information is expected to adhere to the District's procedures and protocols.

DEFINITIONS

1. "Access" is the flow of information between a store of data and a "data user", system, or process. A "data user", system, or process is considered to have access to data if it has one or more of the following privileges: the ability to read or view the data, update, or change the existing data, create new data, delete data, or the ability to make a copy of the data. Access can be provided either on a continual basis or, alternatively, on a one-time or ad hoc basis. Transferring any data from one party to another in any medium is equivalent to permitting access to that data.

2. A "data steward" is the individual responsible for the data. The Data Steward is usually the Chief, department head, or Principal of the school or department that created or originated the data.

3. A "data user" is an individual that has been authorized to "access" data for the performance of his/her job duties.

4. "Institutional Data" is data, regardless of format, maintained by the District or a party acting on behalf of the District for reference or use by multiple District units. Institutional data does not include data that is personal property of a member of the district community, research data, or data created and/or kept by individual employees or affiliates for their own use. Examples of Institutional Data include student education records, payroll records, human resources records, and enterprise directory records.

5. "Sensitive Data" is data that contains information that can be classified as either "sensitive" or "restricted." Some examples of sensitive data include district data that is personally identifiable in nature and contain Social Security Numbers, Credit Card Numbers or other financial account numbers, HIPAA protected health information, or FERPA protected student education records.

POLICY

1. District data shall be classified in accordance with the Data Classification and Protection Standard to identify the level of confidentiality needs, legal requirements, and minimum standard protections for the data before access is granted.

2. The District shall maintain confidential information only in areas where there is a legitimate and justifiable need. When at all possible, confidential information should be accessed from its original source, and copies or printed versions of the information shall be kept to a minimum.

3. The District shall retain data no longer than necessary and consistent with state and federal law.

4. The Board hereby directs the Superintendent to adopt an Administrative Regulation to implement and maintain the purpose of this Board Policy. The Superintendent shall include in the Administrative Regulation the following provisions:

    a. The Superintendent shall designate data stewards, based on their job titles and roles, who may permit access to sensitive data. Access shall be granted in compliance with relevant regulations to include, but not limited to: Family Educational Rights and Privacy Act (FERPA); Individuals with Disabilities in Education (IDEA), Health Insurance Portability and Accountability Act (HIPPA); and the Gramm-Leach-Bliley Act (GLBA).

5. Data users must responsibly use data for which they have access, including only using the data for its intended purpose and respecting the privacy of members of the District community. Data users must maintain the confidentiality of data in accordance with all applicable laws and policies. Authorized access to sensitive data does not imply authorization for copying, further dissemination of data, or any use other than the use for which the employee was authorized. The data steward retains the right to approve and grant access to sensitive data.

6. Data that is identified to particular individuals (e.g., names, student ID numbers, addresses, telephone numbers, etc.) shall be used only within the scope of the individual's responsibilities.

7. Any release of any individual or aggregate student information to anyone other than District employees who have a legitimate educational interest must be authorized by the appropriate District Office in a written request stating the use of the data.

8. Access to student information through the District's Data Warehouse shall be made available only to individuals with a legitimate educational interest.

9. A person who has access to sensitive records may not:

    a. Reveal the content of any record or report to anyone, except in the conduct of their work assignments and in accordance with District policies, regulations, and procedures;

    b. Access sensitive information that is not needed for the performance of their job;

    c. Make or allow any unauthorized use of information in financial data files;

    d. Knowingly include false, inaccurate, or misleading entry in any report or record;

    e. Knowingly expunge a data record or a data entry from a record, report, or file;

    f. Share access codes or passwords with any other person;

    g. Seek personal benefit or allow others to benefit personally from the knowledge of any confidential information they acquired through work assignments; or

    h. Remove any official record or report, or copy of any official report, from the office where it is maintained, except in the performance of official duties.

10. Any knowledge of a violation of this Board Policy must be reported immediately to the violator's supervisor. Violations may lead to disciplinary action, up to and including termination. Violations can also lead to action under federal and state laws pertaining to theft, alteration of public records or other applicable sections.

LEGAL REQUIREMENTS AND ASSOCIATED DOCUMENTS

1. This Board Policy complies with Nevada Revised Statutes (NRS) and Nevada Administrative Code (NAC), to include:

    a. NRS Chapter 239, Public Records;

    b. NRS Chapter 391, Personnel; and

c. NRS Chapter 392, Pupils.

2. This Board Policy complies with federal laws and regulations, to include:
   a. Federal Educational Right to Privacy Act (FERPA);
   b. Individuals with Disabilities in Education Act (IDEA);
   c. Children's Internet Protection Act (CIPA); and
   d. Protecting Children in the 21st Century Act.

REVISION HISTORY

Date	Revision	Modification
06/10/2014	1.0	Adopted
07/26/2022	2.0	Revised: Update format and clarify language