Responsible Office: Office of Information Technology (IT)

BOARD POLICY 7205

INFORMATION TECHNOLOGY – DATA ACCESS POLICY

PURPOSE

It is the intent of the Board of Trustees to ensure the security of all elements of the Washoe County School District's computer systems, related technology, and electronic information; to delineate appropriate uses for all users of the District's computer systems; to promote academic success through the use of computer systems, related technology, and electronic information in a safe environment; and to ensure compliance with relevant state and federal law. The Board of Trustees believes that the security and confidentiality of student and employee records are matters of concern to the Board of Trustees, all District employees, and all other persons who have access to District records. Each individual who has access to confidential information is expected to adhere to the District's procedures and protocols. This policy shall clarify responsibilities in these areas.

POLICY

1. Washoe County School 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. Those levels are classified as follows:

    a. Level 1 – Confidential

        i. Confidential, or sensitive, information is based on criteria including but not limited to:

            1. Disclosure exemptions - Information maintained by the District that is exempt from disclosure under the provisions of Nevada Revised Statutes, Chapter 239, Public Records, or other applicable state or federal laws.

            2. Severe risk - Information whose unauthorized use, access, disclosure, acquisition, modification, loss, or deletion could result in severe damage to the District, its students or staff. Financial loss, damage to the District's reputation, and/or legal action could occur.

3. Limited use - Information intended solely for use within the District and limited to those with a "need-to know."

4. Legal Obligations - Information for which disclosure to persons outside of the District is governed by specific standards and controls designed to protect the information.

ii. Examples of such confidential information include medical records, social security number and name, and passwords or credentials that grant access to level 1 and level 2 data.

b. Level 2 – Internal Use

i. "Internal use" data is based on criteria including but not limited to:

1. Sensitivity - Information which must be protected due to proprietary, ethical, contractual or privacy considerations;

2. Moderate risk - Information which may not be specifically protected by statute, regulations, or other legal obligations or mandates but for which unauthorized use, access, disclosure, acquisition, modification, loss, or deletion of could cause financial loss, damage to the District's reputation, violate an individual's privacy rights, or make legal action necessary.

ii. Examples of such "internal use" information include personally identifiable student educational records not defined as "directory" information under the Federal Educational Right to Privacy Act (FERPA); and information contained in an employee's personnel file.

c. Level 3 – General

i. General information is publically available and/or intended to be provided to the public. Information at this level requires no specific protective measures but may be subject to appropriate review or disclosure procedures at the discretion of the District in order to mitigate potential risks. Disclosure of this information does not expose the District to financial loss or jeopardize the security of the District's information assets; however, damage to the District's reputation could occur.

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. Access to sensitive data is designated by the Superintendent and is linked to job titles and roles (data stewards). Data stewards may include members of the District's Leadership Team, school site principals/administrators, or department heads of the school or department that generated the 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). Data stewards are assigned in the following chart:

Institutional Data	Data Steward	Trusted Designee(s)
Data containing individuals' Social Security Numbers	Chief Financial Officer; Senior Director, Student Accounting; Office of Accountability	IT Applications Staff
Student Records	Senior Director, Student Accounting, Office of Accountability	IT Applications Staff, Office of Accountability Staff
Data Warehouse (BIG)	Chief Information Officer	BI Analysts, IT Coordinator – DBA
Employee Records	Chief Human Resources Officer	IT Applications Staff
Other Data	Originating Units – Department Head, Chief, Principal, Assistant Principal, etc.	None specified

   a. Data stewards shall ensure that procedures for requesting and approving access to sensitive data exist and are followed. This includes implementing procedures for regularly auditing access to sensitive data and revoking access when it is no longer needed or authorized. Procedures may vary as necessary to accommodate different missions, resources, etc., and shall include sufficient tracking of requests, approvals, and revocations so that authorized access to sensitive data is auditable.

   b. All access by individuals to sensitive data shall be controlled by reasonable measures to prevent access by unauthorized users.

   c. All persons who have access to data must adhere to all applicable federal and state laws.

4. 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.

5. A data steward may delegate the ability to approve access to sensitive data to trusted individuals in designated roles. A data steward may delegate by creating procedures through which the designee may approve access by employees that have certain pre-approved job titles, roles and responsibilities. Data stewards retain the responsibility for ensuring that all access to sensitive data is authorized, appropriate, and complies with relevant legal requirements; the responsibility does not transfer to designees.

6. Data that is identified to particular individuals (e.g., inclusion of 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 'need to know' 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 on to individuals with a legitimate educational "need to know".

    a. Staff working at a single school will only have access to the students that attend that school. Staff working over several schools such as Area Superintendents and have a need to know shall have access to multiple and potentially all school data. Staff that work at the district administration level and have a need to know shall have access to all student, staff, and school data.

    b. Access to the data warehouse information is initially granted via the "BIG" portal and is associated to an authorized District domain user ID. Once the user agrees to the Data Confidentiality Agreement, that user will have access to the data that is associated with his/her location and job title. In order to comply with the new performance framework and to allow staff to collaborate and plan effective educational curriculum to meet goals and interventions, all approved staff in a school building will have access to all reported data related to the students in that building. Data that is saved locally must also be adequately protected from outside access. Data

downloaded from the data warehouse and saved locally should be updated frequently so that the likelihood of incorrect data is minimized.

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 his/her work assignments and in accordance with District policies, regulations and procedures.

    b. Access sensitive information that is not needed for the performance of his/her 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 he/she has acquired through work assignments.

    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 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.

DEFINITIONS

1. Access is the flow of information between a store of data and a user, system, or process. A 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. 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.

3. 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.

4. 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.

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

DESIRED OUTCOMES

1. All data that is considered sensitive is managed and secured and all access to that data is granted on a need to know basis.

2. Data stewards are aware of the data under their control and their responsibilities to secure that data and access to it.

3. Data users are aware of their responsibility to secure data regardless of format and how access to data is determined.

IMPLEMENTATION GUIDELINES & ASSOCIATED DOCUMENTS

1. This policy reflects the goals of the District's Strategic Plan.

2. This policy complies with Nevada Revised Statutes (NRS), to include:

    a. Chapter 239, Public Records

    b. Chapter 391, Personnel

    c. Chapter 392, Pupils

3. This 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)

d. Protecting Children in the 21st Century Act

REVIEW AND REPORTING

1. This policy shall be audited annually to ensure its continued relevance. Any suggested revisions shall be considered by the Board of Trustees.

REVISION HISTORY

Date	Revision	Modification
6/10/2014	1.0	Adopted