Policy

INFORMATION SYSTEM

The Hortonville Area School District collects, classifies, and retains data/information from and about students, staff, vendors/contractors, and other individuals, about programs and initiatives undertaken by the school system, and about and related to the business of the District. This information may be in hard copy or digital format, and may be stored in the District or offsite with a third party provider.

Data/information collected by the District shall be classified as Confidential, Controlled, or Published. Data/information will be considered Controlled until identified otherwise.

Protecting District Information Resources (as defined in Bylaw 0100) is of paramount importance. Information security requires everyone's active participation to keep the District's data/information secure. This includes Board members, staff members/employees, students, parents, contractors/vendors, and visitors who use District Technology Resources (as defined in Bylaw 0100) and Information Resources.

Individuals who are granted access to data/information collected and retained by the District must follow established procedures so that the information is protected and preserved. Board members, administrators, and all District staff members, as well as contractors, vendors, and their employees, granted access to data/information retained by the District are required to certify annually that they shall comply with the established information security protocols pertaining to District data/information. Further, all individuals granted access to Confidential Data/Information retained by the District must certify annually that they will comply with the information security protocols pertaining to Confidential Data/Information. Completing the Confidential Agreement found in the staff Handbooks and Criminal History Record Check and Employee Self Reporting Requirements application shall provide this certification.

All Board members, staff members/employees, students, contractors/vendors, and visitors who have access to Board-owned or managed data/information must maintain the security of that data/information and they District Technology Resources on which it is stored.

If an individual has any questions concerning whether this policy applies to them, the individual should contact the District's Technology Director or Information Technology Department/Office.

The District has policies that set forth the internal controls necessary to provide for the collection, classification, retention, access, and security of District Data/Information.

Further, the District Administrator is authorized to develop procedures that would be implemented in the event of an unauthorized release or breach of data/information. These procedures shall comply with the District's legal requirements if such a breach of personally-identifiable information occurs.

Board Approved 6/26/23; 3/10/25
Adoption Resolution 10/13/14

Policy

The District Administrator shall require the participation of staff members in appropriate training related to the internal controls pertaining to the data/information that they collect, to which they have access, and for which they would be responsible for the security protocols.

Third-party contractors/vendors who require access to Confidential Data/Information collected and retained by the District, will be informed of relevant Board policies that govern access to and use of Information Resources, including the duty of safeguarding the confidentiality of such data/information.

Failure to adhere to the policy and its related administrative guidelines may put data/information collected and retained by the District at risk. Employees who violate this policy may have disciplinary conse1uences imposed up to and including termination of employment, and/or referral to law enforcement. Students who violate this Policy will be subject to disciplinary action, up to and including expulsion, and/or referral to law enforcement. Contractors/vendors who violate this policy may face termination of their business relationships with and/or legal action by the District. Parents and visitors who violate this Policy may be denied access to the District's Technology Resources.

The District Administrator will conduct a periodic assessment of risk related to the access to and security of the data/information collected and retained by the District, as well as the viability of the continuity of organizational operations plan developed pursuant to Policy #8300 Continuity of Organizational Operations. Public discussion of any component of an Information Systems assessment or audit will not be held if, at the District Administrator's discretion, doing so would jeopardize cybersecurity, or the confidentiality, integrity, or availability of employee or student information, or any other security related considerations requires confidentiality.

NEOLA 2024

Board Approved 6/26/23; 3/10/25
Adoption Resolution 10/13/14