Book	Policy Manual
Section	READY FOR 3-11-2025
Title	Copy of INFORMATION SECURITY
Code	po8305
Status	
Adopted	August 13, 2019
Last Revised	March 11, 2025
Prior Revised Dates	2/14/2023

8305 - **INFORMATION SECURITY**

The 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 - Definitions) 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 - Definitions) 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.

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 the District *Technology Resources* on which it is stored.

If an individual has any questions concerning whether this ~~Policy~~ policy and/or its related administrative guidelines apply to ~~him/her~~the individual or how ~~they~~this policy and/or related administrative guidelines apply to ~~him/her~~the individual, then the individual should contact the District's Technology Director or Information Technology Department/Office.

[X] The District Administrator shall develop administrative guidelines that set forth the internal controls necessary to provide for the collection, classification, retention, access, and security of District Data/Information.

~~The Superintendent shall develop administrative guidelines that set forth the internal controls necessary to provide for the collection, classification, retention, access, and security of District Data/Information.~~

Further, the ~~Superintendent~~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. ~~.~~ (See Policy 8320.01 - Unauthorized Acquisition of Staff Personal Information and/or Policy 8330.01 - Unauthorized Acquisition of Student Personal Information.)

The ~~Superintendent~~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 to safeguard the confidentiality of such data/information.

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

The ~~Superintendent~~District Administrator shall 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 Plan.~~ 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.

T.C. 2/14/23

Legal

Last Modified by Coleen Frisch on January 28, 2025