Book	Policy Manual
Section	Board Review 38.1
Title	Vol. 38, No. 1 - September 2023 Technical Correction INFORMATION SECURITY
Code	po8305
Status	First reading
Adopted	June 12, 2023
Last Reviewed	November 7, 2023

Technical Correction - Vol. 38, No. 1

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

Protecting District Information & Technology 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 of Education members, staff members/employees, students, parents, contractors/vendors, and visitors who use District Information & Technology Resources (as defined in Bylaw 0100).

Individuals who are granted access to data/information collected and retained by the District must follow established procedures so that the data/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 appropriate section of the Staff Technology Acceptable Use and Safety form (Form 7540.04 F1) 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 the District Information & Technology Resources on which it is stored.

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

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 is charged with developing procedures that can 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.

The Superintendent shall require staff members to participate in training related to the internal controls applicable to the data/information that they collect and have access to and for which they are 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 District Information & Technology Resources, including the duty to safeguard the confidentiality of such data/information.

Failure to adhere to this Policy and its related administrative guidelines may put data/information collected and retained by the District at risk. Employees who violate this policy and/or its related administrative guidelines may be disciplined, up to and including termination of employment and/or referral to law enforcement. Students who violate this Policy and/or its related administrative guidelines will be disciplined, up to and including expulsion and/or referral to law enforcement. **( )** Contractors/vendors who violate this Policy and/or its related administrative guidelines may face termination of their business relationships with and/or legal action by the District. **[END OF OPTION]** Parents and visitors who violate this Policy and/or its related administrative guidelines may be denied access to the District's Information & Technology Resources.

The Superintendent shall conduct a periodic assessment of risk related to the access to and security of the data/information collected and retained by the District.

Cross References
po0100

Cross References	po0100 - DEFINITIONS

Last Modified by Amy Manchester on November 7, 2023