Book	Policy Manual
Section	Board
Title	Cybersecurity
Code	EHC
Status	
Adopted	December 9, 2024

Cybersecurity

To accomplish the District's mission and comply with the law, the District must collect, create and store confidential and critical information. The District must maintain and protect this data for efficient District operations, compliance with laws mandating confidentiality, and maintaining the trust of the District's stakeholders. Individuals with access to District data are required to follow State and Federal law, District policies and procedures created to protect the information.

The Board is concerned with preventing incidents that actually or potentially jeopardize the confidentiality, integrity or availability of an information system or the information that it processes, stores or transmits, and protect against loss of District funds through cybersecurity threats and incidents.

The Board directs the Superintendent/designee to develop procedures to effectively prevent cyberattacks, protect against data loss or breaches, ensure overall safety and security of technology and protect against loss of District funds. Such procedures should include at minimum:

1. Staff training on recognizing attempted cyberattacks including, but not limited to, spear phishing emails. Such training may also be provided to students where deemed appropriate.

2. Measures and training to prevent payment re-direct schemes. Such training must include how to recognize these schemes and include procedures to verify and validate requests prior to any fund transfers, including requiring in-person change requests where appropriate and use of added layers of authentication and security such as those available through the District's financial institutions.

3. Data protection measures to prevent data breaches of confidential information and prompt identification of any breaches that may occur. Such measures will include encryption to the extent feasible. If an employee suspects, discovers and/or determines that a security breach of confidential databases has occurred, the employee must promptly notify their immediate supervisor and the Superintendent. The Superintendent/designee will determine and implement the steps necessary to correct the unauthorized access and notify those individuals whose personal information may have been compromised.

4. Regular risk assessments to identify, assess and prioritize potential cybersecurity risks to District networks and systems.

5. Password procedures that ensure strong passwords and password updates as deemed appropriate.

6. Approval of software and applications, free or paid, used by District staff to ensure the provider complies with all applicable laws regarding data storage and collection and aligns with District's established risk prevention measures.

7. Incident response plans detailing how to respond in the case of a cyberattack, including an analysis of the incident to prevent future incidents.

District staff, students and other authorized users of District networks and data systems are required to comply with established cybersecurity procedures. Failure to comply may result in discipline.

Legal References

Children's Internet Protection Act; 47 USC 254 (h)(5)(b)(iii); (P.L. 106-554, HR 4577, 2000, 114 Stat 2763)
Family Educational Rights and Privacy Act; 20 USC 1232g
Family Educational Rights and Privacy Act; 20 USC 1232h
Individuals with Disabilities Education Act; 20 USC 1400 et seq.
ORC 1347.12

NOTE: *In addition to this policy, districts should develop district-level procedures for management of cybersecurity risks. Districts also should review Auditor of State (AOS) bulletin 2024-03 addressing payment redirect and business email compromise schemes. The bulletin was released to set clear standards and expectations for public entities and employees regarding the handling of requests for payment redirects. Per the bulletin, "failure to follow the guidance in this bulletin may result in an AOS finding when a loss occurs, and the employee is considered liable as a result of negligence or performing duties without reasonable care."*

Legal

Children s Internet Protection Act; 47 USC 254 (h)(5)(b)(iii); (P.L. 106-554, HR 4577, 2000, 114 Stat 2763)

Family Educational Rights and Privacy Act; 20 USC 1232g

Family Educational Rights and Privacy Act; 20 USC 1232h

Individuals with Disabilities Education Act; 20 USC 1400 et seq.

ORC 1347.12