Book	Policy Manual
Section	800 Operations
Title	Data Storage Policy
Code	830.2
Status	Active
Last Revised	April 27, 2023

Purpose

The Board is committed to the secure management of the district's electronic data to ensure the confidentiality, integrity, and the availability of the data for all district users.

Delegation of Responsibility

The Superintendent shall develop procedures to implement this policy, and shall delegate to their designee(s) the right to enforce this policy.

Definitions

Sensitive Electronic Data – electronic data stored by the District that includes student records, employee records, financial records, and any other confidential or sensitive information.

Transitory Electronic Data – temporary electronic data not regularly stored by the District including, but not limited to, website cookie data, social media posts, live chat, deleted messages, and video surveillance that has not been purposefully saved.

Personal Information - An individual's first name or first initial and last name in combination with and linked to any one or more of the following data elements when the data elements are not encrypted or redacted:

i. Social Security number.

ii. Driver's license number or a State identification card number issued in lieu of a driver's license.

iii. Financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account.

iv. Medical Information

v. Health Insurance information.

vi. A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

Guidelines

Data Security Controls

The Superintendent, or their designee, shall utilize appropriate technical controls including firewalls, virus/malware detection, network access controls, user access controls, intrusion detection systems, encryption, and/or regular software updates to maintain the integrity and security of all of the District's electronic data.

Access Controls

Sensitive electronic data shall be accessible to individual users on a need-to- know basis only. The Superintendent, or their designee, shall ensure that technical controls are utilized to effectively restrict access to sensitive electronic data to individuals with a legitimate educational or operational purpose to access such data.

Backups

The Superintendent, or their designee, shall ensure that the District maintains regular and up-to-date backups of all sensitive electronic data, and that such back-ups are stored either offline or are sent to secure off-site storage.

Vendors

The District may engage vendors who will have access to sensitive electronic data. In such cases, the Superintendent, or their designees, shall ensure that the vendor is required to adhere to the same data security standards as outlined in this policy, and shall ensure the appropriate provisions in the vendor contract to ensure compliance.

Data Storage

Sensitive electronic data may only be stored in secure storage approved by the District. The Director of Operations, or their designee, shall maintain a list of approved storage options for sensitive electronic data and shall disseminate such list at least annually to all staff and administrators

Policy____ - Record Retention Policy; AR Record Retention Schedule

Retention

Sensitive electronic data shall be retained in accordance with the District's record retention policy and record retention schedule. Transitory electronic data shall only be maintained as delineated in the record retention schedule.

Personal E-mail

Personal e-mail accounts (accounts not issued by the District) shall not be used to transmit the District's sensitive electronic data in any way (including e- mailing files to/from one's own District e-mail account).

Personal Electronic Devices

Policy____ - Employee Mobile Device Policy

Employees should exercise caution, and utilize appropriate security measures such as password protection on their personal electronic device, to prevent any unauthorized access to sensitive electronic data. In no case shall employees store sensitive electronic data locally on the hard drive or internal memory of the employee's personal electronic device.

Data Breach

Any actual or suspected data breach (including unauthorized access to sensitive electronic data or exceeding one's authorization to electronic data) must be immediately reported to the Director of Technology.

Data Breach

Any actual or suspected data breach (including unauthorized access to sensitive electronic data or exceeding one's authorization to electronic data) must be immediately reported to the Director of Technology.

Any data breach that results in unauthorized access to unredacted and unencrypted personal information shall be immediately reported to the Superintendent. The Superintendent, or their designee shall follow the notification procedures required by the Breach of Personal Information Notification Act.

Risk Assessments

The Director of Operations, or their designee, shall conduct regular vulnerability and risk assessments to monitor compliance with this policy.

Penalties for Violations

Violations of this policy, other Board policies, administrative regulations, and/or state or federal laws, including unauthorized access to sensitive electronic data, will result in discipline, up to and including dismissal. If appropriate, referrals will be made to law enforcement officials.

Development of Administrative Guidelines

The Superintendent or their designee may develop administrative guidelines to implement this policy. The Superintendent shall ensure that all students and employees are made aware of this policy and any administrative guidelines by means of the employee and student handbooks, the school district website, or other reasonable means.

73 Pa. Stat. §2301 et seq.