DATA GOVERNANCE

The board of education believes that data or information in all its forms - written, electronic, recorded or printed – must be protected from accidental or intentional unauthorized modification, destruction or disclosure throughout its life cycle. This protection shall include an appropriate level of security over the equipment, digital code, and practices used to process, store, and transmit data or information.

The chief school administrator or his or her designee shall establish, implement, and maintain data and information security measures. Board policy and district procedures shall apply to all students and employees of the district, contractual third parties and agents of the district, and volunteers who have access to district data systems or data. This policy applies to all forms of data and information, including but not limited to:

A. Speech, spoken face to face, or communicated by phone or any current and future technologies;

B. Hard copy data printed or written, communications sent by post/courier, fax, electronic mail, text, chat and or any form of social media, etc.;

C. Data stored and/or processed by servers, PC's, laptops, tablets, mobile devices, etc.; and

D. Data stored on any type of internal, external, or removable media or cloud based services.

The data governance policies and procedures shall be reviewed regularly by the data governance committee.

Annual training shall be conducted on the district data governance policy and procedures.

Risk Management

The risk assessment shall be used as a basis for a plan to mitigate identified threats and risk to an acceptable level. The chief school administrator or his or her designee shall administer periodic risk assessments to identify, quantify, and prioritize risks.

Data Classification

Data shall be classified in order to promote proper controls for safeguarding the confidentiality of data. Regardless of classification the integrity and accuracy of all classifications of data shall be protected. The classification assigned and the related controls applied shall be dependent on the sensitivity of the data. Data shall be classified according to the most sensitive detail they include. Data recorded in several formats (e.g., source document, electronic record, report) have the same classification regardless of format.

Systems and Information Control

Any computer, laptop, mobile device, printing and/or scanning device, network appliance/equipment, AV equipment, server, internal or external storage, communication device or any other current or future electronic or technological device may be referred to as systems. All involved systems and information are assets of district and shall be protected from misuse, unauthorized manipulation, and destruction. These protection measures may be physical and/or code-based. All technological applications are considered “digital code” in this document.

DATA GOVERNANCE (continued)

A. Ownership of Digital Code:

All digital code developed by district employees or contract personnel on behalf of the district and all digital code licensed or purchased for the district schools use is the property of board and shall not be installed for use at home or any other location, unless otherwise specified by the license agreement.

B. Digital Code Installation and Use:

All digital code that reside on technological systems within or used by the district schools shall comply with applicable licensing agreements and restrictions and shall comply with the district acquisition of digital code procedures.

C. Virus, Malware, Spyware, Phishing, Ransomware, and SPAM Protection:

Virus checking systems approved by the director of technology shall be deployed using a multi-layered approach (computers, servers, gateways, firewalls, filters, etc.) that ensures all electronic file are appropriately scanned for viruses, malware, spyware, phishing, ransomware, and SPAM. Users shall not delete or disable district protection systems or install other similar systems.

D. Access Controls:

Physical and electronic access to information systems that contain personally identifiable information (PII), confidential information, internal information and computing resources shall be controlled. To ensure appropriate levels of access by internal workers, a variety of security measures shall be instituted as approved by the chief school administrator.

1. Identification/Authentication: Unique user identification (user ID) and authentication shall be required for all systems that maintain or access personally identifiable information (PII), confidential information, and/or internal information. Users shall be held accountable for all actions performed on the system with their user ID. User accounts and passwords shall NOT be shared.

2. Transmission Security: Technical security mechanisms shall be implemented to guard against unauthorized access to data that are transmitted over a communications network, including wireless networks. The following features are implemented:

    a. Integrity controls; and
    b. Encryption, where deemed appropriate.

    Note: Only district-supported email accounts shall be used for communications to and from school employees, to and from parents or other community members, to and from other educational agencies, to and from vendors or other associations, and to and from students for school business.

    Remote Access: Access into the district network from outside shall only be allowed through methods authorized by the director of technology. All other network access options are strictly prohibited without explicit authorization from the director of technology. Personally identifiable information, confidential information and/or internal information that is stored or accessed remotely shall be maintained with the same level of protections as information stored and accessed within the district network. Personally identifiable information shall only be stored in cloud storage if said storage has been approved by the data governance committee or its designees.

3. Physical and Electronic Access and Security: Access to areas in which information processing is carried out shall be restricted to only appropriately authorized individuals.

DATA GOVERNANCE (continued)

a. No personally identifiable information, confidential and/or internal information shall be stored on a device's internal storage, a mobile device of any kind, or an external storage device that is not located within a secure area.
b. No personally identifiable information shall be stored in personal cloud storage.
c. No technological systems that may contain information as defined above shall be disposed of or moved without adhering to the appropriate Purchasing and Disposal of Electronic Equipment procedures.
d. It is the responsibility of the user to not leave these devices logged in, unattended, and open to unauthorized use.

Electronic Mass Data Transfers

Downloading, uploading or transferring personally identifiable information, confidential information, and internal information between systems shall be strictly controlled. Requests for mass download of, or individual requests for, information for research or any other purposes that include personally identifiable information shall be in accordance with law, with this policy and be approved by the chief school administrator.

All other mass downloads of information shall be approved by the director of technology and include only the minimum amount of information necessary to fulfill the request. A Memorandum of Agreement (MOA) or equivalent shall be in place when transferring personally identifiable information to external entities such as software or application vendors, textbook companies, testing companies, or any other web based application, etc. unless the exception is approved by the chief school administrator.

Personally identifiable information, confidential information, and internal information shall be stored in a manner inaccessible to unauthorized individuals. Personally identifiable information and confidential information shall not be downloaded, copied or printed indiscriminately or left unattended and open to compromise. Personally identifiable information that is downloaded for educational purposes where possible shall be redacted before use.

Oral Communications

District employees shall be aware of their surroundings when discussing personally identifiable information and confidential information. This includes but is not limited to the use of cellular telephones in public areas. District employees shall not discuss personally identifiable information or confidential information in public areas if the information can be overheard. Caution shall be used when conducting conversations in: semi-private rooms, waiting rooms, corridors, elevators, stairwells, cafeterias, restaurants, or on public transportation.

Evaluation

Periodic technical and nontechnical evaluations shall be conducted of access controls, storage, and other systems. Appropriate measures to ensure continued protection shall be implemented to respond to environmental or operational changes affecting the security of electronic personally identifiable information.

Disaster Recovery

A disaster recovery plan shall be developed and implemented for prompt and efficient recovery from damage to critical systems, data, or information. Each school, department, and individual shall be required to report any system emergency or other occurrence (for example, fire, vandalism, system failure and natural disaster) that may damages data or systems instances immediately to the chief school administrator and the director of technology. The disaster recovery plan shall include the following:

A. A prioritized list of critical services, data, and contacts;

B. A process enabling the district to restore any loss of data in the event of fire, vandalism, natural disaster, or system failure;

C. A process enabling the district to continue to operate in the event of fire, vandalism, natural disaster, or system failure;

D. Procedures for periodic testing of written contingency plans to discover weaknesses and the subsequent process of revision the documentation, if necessary.

Compliance

This policy shall apply to all users of the district network information including: employees, staff, students, volunteers, and outside affiliates. Employees and volunteers failing to comply with this policy may subject to disciplinary measures up to and including termination of employment or assignment. Outside affiliates violating this policy may be subject to termination of affiliation. Students violating this policy may be subject to disciplinary actions consistent with the code of student conduct (see board policy 5131 Conduct and Discipline). Penalties associated with state and federal law may also apply.

The following actions are specifically prohibited and shall be grounds for disciplinary measures, including but not limited to:

A. Unauthorized disclosure of personally identifiable information or confidential information;

B. Unauthorized disclosure of a log-in code (User ID and password);

C. Any attempt to obtain a log-in code or password that belongs to another person;

D. Any attempt to use another person's log-in code or password;

E. Unauthorized use of an authorized password to invade student or employee privacy by examining records or information for which there has been no request for review;

F. Installation or use of unlicensed digital code on the district technological systems;

G. The intentional unauthorized altering, destruction, or disposal of district information, data and/or systems. This includes the unauthorized removal from district technological systems such as but not limited to laptops, internal or external storage, computers, servers, backups or other media, copiers, etc. that contain personally identifiable information or confidential information;

H. Any attempt to gain access to log-in codes for purposes other than for support by authorized technology staff, including the completion of fraudulent documentation to gain access.

NJSBA: February 2019
Adopted: May 2, 2019

Key Words

Digital, Technology, Technological, Network, Data Recovery, Security, Technological System

Legal References:		
	N.J.S.A. 2A:4A-60 et al.	Disclosure of juvenile information; penalties for disclosure
	N.J.S.A. 2A:38A-1 et seq.	Computer System
	N.J.S.A. 2C:20-25	Computer Related Theft
	N.J.S.A. 18A:7A-10	NJQSAC

DATA GOVERNANCE (continued)

N.J.S.A. 18A:36-19	Pupil records; creation, maintenance and retention, security and access; regulations; nonliability
N.J.S.A. 18A:36-35	School Internet websites; disclosure of certain student information prohibited
N.J.S.A. 18A:36-39	Notification by school to certain persons using certain electronic devices; fine
N.J.S.A. 47:1A-1 et seq.	Examination and copies of public records (Open Public Records Act)
N.J.S.A. 47:3-15 et seq.	Destruction of Public Records Law
N.J.A.C. 6A:8-4.2	Documentation of student achievement
N.J.A.C. 6A:14-1.1 et seq.	Special Education
See particularly: N.J.A.C. 6A:14-1.3, -2.3, -2.9, -7.9	
N.J.A.C. 6A:16-1.1 et seq.	Programs to Support Student Development
See particularly: N.J.A.C. 6A:16-1.4, -2.2, -2.4, -3.2, -5.4, -6.5, -10.2	
N.J.A.C. 6A:30-1.1 et seq.	Evaluation of the Performance of School Districts
N.J.A.C. 6A:32-2.1	Definitions
N.J.A.C. 6A:32-7.1 et seq.	Student records
N.J.A.C. 6A:32-8.1	School register
N.J.A.C. 8:61-2.1	Attendance at school by students or adults infected by Human Immunodeficiency Virus (HIV)
N.J.A.C. 15:3-2	Records retention
N.J.A.C. 6A:30-1.1et seq.	Evaluation of the Performance of School Districts
N.J.A.C. 6A:32-2.1	Definitions
N.J.A.C. 6A:32-7.1 et seq.	Student records

20 U.S.C.A. 1232g - Family Educational and Privacy Rights Act

47 U.S.C. 254(h) - Children's Internet Protection Act

16 CFR, Part 312 - Children's Online Privacy Protection Act

Possible Cross References:

*1000/1010	Concepts and Roles in Community Relations
*1100	Communication with the Public; and
*1111	District Publications
*3000	Concepts and Roles in Business
*3100	Budget Planning Preparation and Adoption
*3300	Purchasing
*3510	Operation and Maintenance of Plant
*3600	Evaluation of Business and Noninstructional Operations
*3570	District records and reports
*5124	Reporting to parents/guardians
*4131/4131.1	Professional Development
*6141	Curriculum design and development
*9322	Public and executive sessions

*Indicates policy is included in the Critical Policy Reference Manual.