HOBOKEN BOARD OF EDUCATION
ESTABLISHED 1850

Data Privacy, Classification and Security Policy 2360.1

Purpose

Data and information are important assets of the District and must be protected from loss of integrity, confidentiality, or availability in compliance with District policy and guidelines, and state and federal laws and regulations.

Scope

This policy applies to all District schools, departments, and affiliated organizations. For the purposes of this policy, affiliated organization refers to any organization associated with the District that uses District information technology resources to create, access, store, or manage District data. These organizations might include assessment providers, food service providers, and online content providers. It also applies to any third party vendor creating, storing, or maintaining District data per a contractual agreement.

Policy

All District Data must be classified according to the Data Classification Schema and protected according to Data Security Standards. This policy applies to data in all formats or media.

Data Classification Schema

Data and information assets are classified according to the risks associated with data being stored or processed. Data with the highest risk need the greatest level of protection to prevent compromise; data with lower risk require proportionately less protection. Three levels of data classification will be used to classify District Data based on how the data are used, its sensitivity to unauthorized disclosure, and requirements imposed by external agencies.

Data are typically stored in aggregate form in databases, tables, or files. In most data collections, highly sensitive data elements are not segregated from less sensitive data elements. For example, a student information system will contain a student's directory information as well as their social security number. Consequently, the classification of the most sensitive element in a data collection will determine the data classification of the entire collection.

District Data Classifications -

A. **Public** - Data explicitly or implicitly approved for distribution to the public without restriction. It can be freely distributed without potential harm to the District, third party systems, or individuals. Public data generally have a very low sensitivity since by definition there is no such thing as unauthorized disclosure, but it still warrants protection since the integrity of the data can be important. Examples include:

1. District's public web site.
2. Directory information for students, faculty, and staff except for those who have requested non-disclosure (e.g., per the Family Educational Rights and Privacy Act (FERPA) for students).
3. Course descriptions.
4. Press releases.
5. Board of Education meeting agendas and minutes.
6. Employee salaries.

B. **Internal** - Data intended for internal District business use only with access restricted to a specific workgroup, department, group of individuals, or third party systems with a legitimate need. Internal data are generally not made available to parties outside the District community. Unauthorized disclosure could adversely impact the District, affiliates, or individuals. Internal data generally have a low to moderate sensitivity. Examples include:

1. Student ID numbers.
2. Employee ID numbers.
3. Student educational records.
4. Information technology transaction logs.
5. Directory information for students, faculty, and staff who have requested non-disclosure (e.g., per FERPA for students.

C. **Confidential**- Highly sensitive data intended for limited, specific use by a department or group of individuals with a legitimate need-to-know. Explicit authorization by the Data Steward is required for access because of legal, contractual, privacy, or other constraints. Unauthorized disclosure could have a serious adverse impact on functions of the District or third party systems, the personal privacy of individuals, or on compliance with federal or state laws and regulations or District contracts. Confidential data have a very high level of sensitivity. Examples include:

1. Social Security Number.
2. Personally identifiable information (PII). The Family Educational Rights and Privacy Act (FERPA) (see 20 U.S.C. §1232g and 34 CFR Part 99) protects personally identifiable information (PII) from students' education records from unauthorized disclosure. FERPA defines education records as "records that are: (1) directly related to a student; and (2) maintained by an educational agency or institution or by a party acting for the agency or institution" (see 34 CFR § 99.3 definition of "education record"). FERPA also defines the term PII, which includes direct identifiers (such as a student's or other family member's name) and indirect identifiers (such as a student's date of birth, place of birth, or mother's maiden name (see 34 CFR § 99.3 definition of "personally identifiable information"). In addition, N.J.S.A. 18A:36-35 defines PII as student names, student photos, student addresses, student e-mail addresses, student phone numbers, and locations and times of class trips.
3. Personnel records.
4. Security information (location of cameras, recordings, lockdown procedures, school or district security plan, details regarding Information technology network structure).

5. Authentication tokens (e.g., personal digital certificates, passwords,).

Data System Inventory - The District maintains an inventory of hosted and subscribed data systems. The inventory contains:

1. Name of data system
2. Function of data system
3. Identification of data steward
4. Type of data stored on the system
5. District policy/rule governing the data stored on the system
6. Link to data system's privacy policy
7. Date of most recent policy review

The inventory includes local and third party systems that have access to school/district data. A public version of the inventory will be posted on the district website for parental access.

Responsible Use of District Data - All data users shall follow guidelines set forth in HBOE Policy 2360 - Acceptable Use of Computer Networks/Computers and Resources (M) and in the district Data Governance Plan.

Data Accessibility Based on Classification or Role

The following table defines required safeguards for protecting data and data collections based on their classification.

In addition to the following data security standards, any data covered by federal or state laws or regulations or contractual agreements must meet the security requirements defined by those laws, regulations, or contracts.

Security Control Category	**Data Classification**		
	Public	**Internal**	**Confidential**
Access Controls	No restriction for viewing. Authorization by Data Steward or designee required for modification; supervisor approval also required if not a self-service function.	Viewing and modification restricted to authorized individuals as needed for business-related roles. Data Steward or designee grants permission for access, plus approval from supervisor. Authentication and authorization required for access	Viewing and modification restricted to authorized individuals as needed for business-related roles. Data Steward or designee grants permission for access, plus approval from supervisor. Authentication and authorization required for access. Confidentiality agreement required.
Copying/Printing (applies to both paper and electronic forms)	No restrictions.	Data should only be printed when there is a legitimate need. Copies must be limited to individuals with a need to know. Data should not be left unattended on a printer.	Data should only be printed when there is a legitimate need. Copies must be limited to individuals authorized to access the data and have signed a confidentiality agreement. Data should not be left unattended on a printer. Copies must be labeled

			"Confidential".
Network Security	May reside on a public network. Protection with a firewall recommended.	Protection with a network firewall required. IDS/IPS protection required. Protection with router ACLs optional. Servers hosting the data should not be visible to entire Internet. May be in a shared network server subnet with a common firewall ruleset for the set of servers.	Protection with a network firewall using "default deny" rule set required. IDS/IPS protection required. Protection with router ACLs optional. Servers hosting the data cannot be visible to the entire Internet, nor to unprotected subnets and guest wireless networks. Must have a firewall ruleset dedicated to the system.
System Security	Must follow general best practices for system management and security. Host-based software firewall recommended.	Must follow District-specific and OS-specific best practices for system management and security. Host-based software firewall required. Host-based software IDS/IPS recommended	Must use district-provided software and hardware to access confidential data. Host-based software firewall required. Host-based software IDS/IPS recommended.

Virtual Environments	May be hosted in a virtual server environment. All other security controls apply to both the host and the guest virtual machines.	May be hosted in a virtual server environment. All other security controls apply to both the host and the guest virtual machines. Should not share the same virtual host environment with guest virtual servers of other security classifications.	May be hosted in a virtual server environment. All other security controls apply to both the host and the guest virtual machines. Cannot share the same virtual host environment with guest virtual servers of other security classifications.
Physical Security	System must be locked or logged out when unattended. Host-based software firewall recommended.	System must be locked or logged out when unattended. Hosted in a secure location required; a Secure Data Center is recommended.	System must be locked or logged out when unattended. Hosted in a Secure Data Center required.
Remote Access to systems hosting the data	No restrictions.	Access restricted to local network or general District Virtual Private Network (VPN) service. Remote access by third party for technical support limited to authenticated, temporary access via direct dial-in modem or secure protocols over the Internet.	Restricted to local network or secure VPN group. Unsupervised remote access by third party for technical support not allowed.
Data Storage	Storage on a secure server recommended. Storage in a secure Data Center recommended.	Storage on a secure server recommended. Storage in a secure Data Center recommended. Should not store on an individual's workstation or a	Storage on a secure server required. Storage in Secure Data Center required. Paper/hard copy: do not leave unattended where others may see it; store in a secure

		mobile device.	location.
Transmission	No restrictions.	No requirements	Encryption required (e.g., via SSL or secure file transfer protocols). Cannot transmit via e-mail unless encrypted and secured with a digital signature.
Backup/ Disaster Recovery	Backups required; daily backups recommended.	Daily backups required. Off-site storage recommended.	Daily backups required. Off-site storage in a secure location required.
Media Sanitization and Disposal (hard drives, CDs, DVDs, tapes, paper, etc.)	No restrictions.	Paper: shred and dispose through a secure shredding service. Hard drives: shred and dispose through a secure shredding service.	Paper: shred and dispose through a secure shredding service. Hard drives: shred and dispose through a secure shredding service.
Training	General security awareness training recommended. System administration training recommended.	General security awareness training required. System administration training required. Data security training required.	General security awareness training required. System administration training required. Data security training required. Applicable policy and regulation training required.

Audit Schedule	As needed.	As needed.	Annual

Note: The table above is adapted from the University of Missouri, Information Security, Data Classification System.

Contracts with Third Parties

Contracts between the District and third parties involving District Data must include language requiring compliance with all applicable laws, regulations, and District policies related to data and information security; immediate notification of the District if District data is used or disclosed in any manner other than allowed by the contract; and, to the extent practicable, mitigate any harmful effect of such use or disclosure.

Roles and Responsibilities

Everyone with any level of access to District Data has responsibility for its security and is expected to observe requirements for privacy and confidentiality, comply with protection and control procedures, and accurately present the data in any type of reporting function. Roles and responsibilities are defined in our Data Governance Plan.

Related Laws, Regulations, or Policies

Hoboken Board of Education Policies -

A. 2361 - Acceptable Use of Computer Networks/Computers and Resources (M)
B. 2360 - Use of Technology (General)
C. 8310 – Public Records
D. 8320 – Personnel Records
E. 8330 – Student Records (M)
F. 8335 - Family Educational and Rights and Privacy Act
G. 5308 – Student Health Records (M)

State of New Jersey

A. N.J.A.C. 6A:16-2.4 et seq.
B. N.J.A.C. 6A:32-7.1. et seq
C. N.J.A.C. 6A:32-7.4 et seq.
D. N.J.A.C. 6A:32-7.5 et seq.
E. N.J.S.A. 10:4-14
F. N.J.S.A. 18A:18A-14.2; 18A:40-19; 18A:66-32; 18A:36-35;
G. N.J.S.A. 18A:36-19a
H. N.J.S.A. 47:1A-1 et seq.

Federal Legislation and Guidelines

A. Family Educational Rights and Privacy Act of 1974 (FERPA)
B. COPPA
C. CIPA
D. ESSA
E. Health Insurance Portability and Accountability Act of 1996 (HIPAA)
F. Electronic Communications Privacy Act of 1986 (ECPA)

Sources:

Kansas State University's Data Security and Classification Policy

Agenda Item Details

Meeting	Jun 11, 2019 - AGENDA
Category	7. ACTION - POLICIES
Subject	7.01 Approval of 2nd Reading of Policy #2360.1 Data Privacy, Classification and Security Procedure
Type	Action (Consent)
Recommended Action	RESOLVED, that the Board of Education, upon recommendation of the Superintendent, approve the second reading of Policy #2360.1 Data Privacy, Classification and Security Procedure.

Motion & Voting

RESOLVED, that the Board of Education approves a Consent Agenda.

Motion by Melanie Tekirian, second by Chetali Khanna.
Final Resolution: Motion Carries
Yes: Malani Cademartori, Sheillah Dallara, Alex De La Torre, Jennifer Evans, Chetali Khanna, Thomas Kluepfel, Melanie Tekirian, Sharyn Angley