Hackensack Public Schools

Data Privacy and Security Guidelines

Updated May 2018

Table of Contents

Purpose

Digital learning has transformed the teaching and learning process by giving both teachers and students easy access to information and resources previously unavailable. However, this transformation has also raised new concerns regarding the privacy and protection of student data in an interconnected world.

There are existing legal and ethical restrictions that apply to districts, schools, and teachers regarding the collection, use and dissemination of student data and education records. Traditionally, student data consisted of attendance, grades, discipline records, and health records and access to that data was restricted to relevant District and/or school personnel such as administrators, guidance counselors, teachers, or other school officials who needed it to serve the educational needs of the child. However, with the rapid growth of educational technology, traditional data is now often shared with companies that provide Student Information Systems (SIS), Learning Management Systems (LMS), and many other technologies and services. As a result, there have been laws enacted and amended governing how and what information is collected or shared, and for what purpose.

Scope

This policy applies to all District schools, offices, departments and affiliated organizations including all employees, students, consultants, vendors and Trustees. 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 including but not limited to assessment providers, food service providers, tutoring service providers, after school programs, etc. It also applies to any third party vendor creating, storing, or maintaining District Data per a contractual agreement.

Effective Date

All new systems designed and implemented after July 1, 2018, must comply with the standards in the "Data Security Standards" section below as well as with any additional requirements set forth in Appendix I if a third-party is involved.

Data stewards must have a compliance plan for all systems with confidential data by October 1, 2019.

Policy

All District Data must be classified according to the Data Classification Schema below and protected according to applicable 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 more sensitive information such as the student’s birthdate and home address. Consequently, the classification of the most sensitive element in a data collection will determine the data classification of the entire collection.

Data Visibility 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, affiliates, 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/Public Session Minutes
    6. Employee Salaries

B. **Sensitive** - Data intended for internal District business use only with access restricted to a specific workgroup, department, group of individuals, or affiliates with a legitimate need. Internal data are generally not made available to parties outside the District but may be subject to FOIA/OPRA Requests. Unauthorized disclosure could adversely impact the

District, affiliates, or individuals. Internal data generally have a low to moderate sensitivity. Examples include:

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

C. **Confidential** - Highly sensitive data intended for limited, specific use by a workgroup, 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 the District or affiliates, the personal privacy of individuals, or on compliance with federal or state laws and regulations. Confidential data have a very high level of sensitivity. Examples include:

1. Social Security Number
2. Personal identity information (PII).
    i. 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").
    ii. N.J.S.A. 18A:36-35 defines "personally identifiable information" 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 (i.e., School Security Plans, camera locations, recordings, Drill schedules, etc.)
5. Authentication tokens (e.g., personal digital certificates, passwords, pin numbers, biometric data)

For a more comprehensive list of examples, please refer to Appendix II on page 24.

Data Security Standards

The following table defines required safeguards for protecting data and data collections based on their classification. Data security requirements for Proprietary Data are determined by the contracting agency and are therefore not included in the table below.

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	**Sensitive**	**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.

Security Control Category	Data Classification		
	Public	Sensitive	Confidential
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".

Security Control Category	Data Classification		
	Public	**Sensitive**	**Confidential**
Network Security	• May reside on a public network. • Protection with a firewall recommended. • IDS/IPS protection recommended. • Protection only with router ACLs acceptable.	• 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. • Servers hosting data accessible via a web server (IIS, Apache, Tomcat, etc.) must be protected with a valid SSL certificate and limit access to HTTPS traffic only. • 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" ruleset 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. • The firewall ruleset should be reviewed periodically. • Servers hosting data accessible via a web server (IIS, Apache, Tomcat, etc.) must be protected with a valid SSL certificate and limit access to HTTPS traffic only.

Security Control Category	Data Classification		
	Public	**Sensitive**	**Confidential**
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 • Servers hosting data accessible via a web server (IIS, Apache, Tomcat, etc.) must be protected with a valid SSL certificate and limit access to HTTPS traffic only.	• 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. • Servers hosting data accessible via a web server (IIS, Apache, Tomcat, etc.) must be protected with a valid SSL certificate and limit access to HTTPS traffic only.
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.

Security Control Category	Data Classification		
	Public	**Sensitive**	**Confidential**
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. • Physical access must be monitored, logged, and limited to authorized individuals 24x7.
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 secure protocols.	• Restricted to local network or secure VPN group. • Unsupervised remote access by third party for technical support not allowed. • Two-factor authentication required.

Security Control Category	Data Classification		
	Public	**Sensitive**	**Confidential**
Data Storage	• Storage on a secure server recommended. • Storage in a secure Data Center recommended. • Storage on District-approved “cloud-based” applications permitted.	• Storage on a secure server recommended. • Storage in a secure Data Center recommended. • Should not be stored on an individual's workstation, mobile device or other portable storage. • Data encryption recommended. • Storage on District-approved “cloud-based” applications permitted (Multi-factor authentication highly recommended).	• Storage on a secure server required. • Storage in Secure Data Center required. • Should not store on an individual workstation or mobile device (e.g., a laptop computer); if stored on a workstation or mobile device, must use whole-disk encryption. • Encryption on backup media required. • AES Encryption required with 256-bit or longer key. • Paper/hard copy: do not leave unattended where others may see it; store in a secure location. • Storage on “cloud-based” applications <u>not permitted</u>.
Transmission	• No restrictions.	• Encryption highly recommended (e.g., via SSL or secure file transfer protocols).	• Encryption required (e.g., via SSL or secure file transfer protocols). • Cannot transmit via e-mail unless encrypted and secured with a digital signature.

Security Control Category	Data Classification		
	Public	**Sensitive**	**Confidential**
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.)	• Please see “Best Practices for Data Destruction” from the Privacy Technical Assistance Center as well as the NIST Special Publication 800-88 Guidelines for Media Sanitization. • Paper: no restrictions.	• Please see “Best Practices for Data Destruction” from the Privacy Technical Assistance Center as well as the NIST Special Publication 800-88 Guidelines for Media Sanitization..	• Please see “Best Practices for Data Destruction” from the Privacy Technical Assistance Center as well as the NIST Special Publication 800-88 Guidelines for Media Sanitization.
Training	• General security awareness training recommended. • System administration training recommended.	• General security awareness training required. • System administration training required. • All employees must pass criminal background check in accordance with State law. • Data security training required.	• General security awareness training required. • System administration training required. • All employees must pass criminal background check in accordance with State law. • Data security training required. • Applicable policy and regulation training required. • Confidentiality Agreement Required.

Security Control Category	Data Classification		
	Public	Sensitive	Confidential
Audit Schedule	• As needed	• As needed	• Annual
Breach Response	• Notification: None required.	• Follow “Hackensack Public Schools Information Security Incident Response Guide”	• Follow “Hackensack Public Schools Information Security Incident Response Guide”

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. For more detailed requirements, please refer to Appendix I.

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. The following roles have specific responsibilities for protecting and managing District Data and Data Collections:

A. **Chief Data Steward -** Senior administration of the District responsible for overseeing all information resources (e.g., Superintendent, Assistant Superintendent, Business Administrator).

B. **Data Steward -** Principals, assistant principals, and heads of academic, administrative, or affiliated departments or their designees with responsibility for overseeing a collection (set) of District Data. They are in effect the owners of the data and therefore ultimately responsible for its proper handling and protection. Data Stewards are responsible for ensuring the proper classification of data and data collections under their control, granting data access permissions, appointing Data Managers for each District Data collection, making sure people in data-related roles are properly trained, and ensuring compliance with all relevant policies and security requirements for all data for which they have responsibility.

C. **Data Governance Team -** A group of Data Stewards appointed by the Chief Data Steward(s) and the Chief Information Security Officer to maintain the data classification schema and standards, set overall data policy, assign a Data Steward to each system and resolve data classification, ownership and integrity issues.

D. **Data Processor -** Individuals authorized by the Data Steward or designee and enabled by the Data Manager to enter, modify, or delete District Data. Data Processors are accountable for the completeness, accuracy, and timeliness of data assigned to them.

E. **Data Viewer** - Anyone in the District or community with the capacity to access District Data but is not authorized to enter, modify, or delete it.

F. **Chief Information Security Officer -** Provides advice and guidance on information and information technology security policies and standards.

G. **Internal Audit Team -** Performs audits for compliance with data classification and security policy and standards.

Collection/Use of District Data

Collection/Use of District Data must not violate any applicable State and Federal Laws and Regulations or District Policies and must be of professional or academic relevance to the role of the individual collecting or using the Data. Data use for non-District purposes such as for external studies/research must be approved by the Superintendent and should consist of de-identified/anonymous data.

Sharing/Transfer of District Data

All sharing/transferring of District data must comply with the relevant data security standards for the highest level of classification of data involved and any applicable State and Federal laws and regulations.

Approved Third-Party Services

Use of third party services that require any District data within the scope of this policy, must be approved by the App Review Committee or Chief Information Security Officer prior to use.

For a list of approved services, please visit: http://goo.gl/nhyds3

Training

To ensure compliance with the data security and privacy standards set forth in this policy, all staff with access to District Data and/or the District network will be provided training opportunities during orientation and on an annual basis. All staff will be required to sign a copy of this policy along with District Acceptable Use policies (2360-2361) acknowledging they have read, understood and will comply with the terms of each policy. Data privacy and security will also be embedded in all District training opportunities that may involve the collection or use of data.

Definitions

Education records - Records that are directly related to a student and are maintained by an educational agency or institution or by a party acting for the agency or institution. For more information, see the Family Educational Rights and Privacy Act regulations, 34 CFR §99.3.

Personally identifiable information (PII) - Information that can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information. See Family Educational Rights and Privacy Act regulations, 34 CFR §99.3, for a complete definition of PII specific to education records and for examples of other data elements that are defined to constitute PII.

ACL - Access Control List; a set of rules in a network device, such as a router, that controls access to segments of the network. A router with ACLs can filter inbound and/or outbound network traffic similar to a firewall but with less functionality.

Authentication - Process of verifying one's digital identity. For example, when someone logs into Webmail, the password verifies that the person logging in is the owner of the eID. The verification process is called authentication.

Authorization - Granting access to resources only to those authorized to use them.

Availability - Ensures timely and reliable access to and use of information.

Confidentiality - Preserves authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Firewall - A specialized hardware and/or software system with stateful packet inspection that filters network traffic to control access to a resource, such as a database server, and thereby provide protection and enforce security policies. A router with ACLs is not considered a firewall for the purposes of this document.

IDS - Intrusion Detection System; a system that monitors network traffic to detect potential security intrusions. Normally, the suspected intrusions are logged and an alert generated to notify security or system administration personnel.

Integrity - Guards against improper modification or destruction of information, and ensures non-repudiation and authenticity.

IPS - Intrusion Prevention System; an IDS with the added ability to block malicious network traffic to prevent or stop a security event.

Local Network - Any segment the District's data network physically located in any District building with an IP address starting with 10.X.X.X or an un-routable private IP address (e.g., 192.X.X.X).

Remote Access - Accessing the District's local network from any physical location outside the Local Network. This includes access from off campus using the District's VPN service.

Secure Data Center - A facility managed by full-time IT professionals for hosting computer, data storage, and/or network equipment with 24x7 auditable restricted access, environmental controls, power protection, and network firewall protection.

Secure Server - a computer that provides services to other computers, applications, or users; is running a server operating system; and is hardened according to relevant security standards, industry best practices, and District security policies.

Sensitivity - Indicates the required level of protection from unauthorized disclosure, modification, fraud, waste, or abuse due to potential adverse impact on an individual, group, institution, or affiliate. Adverse impact could be financial, legal, or on one's reputation or competitive position. The more sensitive the data, the greater the need to protect it.

De-identified/Anonymous Data - The District/User has removed all personally identifiable information and there is a reasonable determination that the student is not identifiable.

District Data - Any data related to Hackensack Board of Education ("District") functions that are:

A. Stored on District information technology systems (internal and hosted).
B. Maintained by District staff or students.
C. Related to institutional processes on or off campus. This applies to any format or media (in other words, it is not limited to electronic data).

VPN - Virtual Private Network; a VPN provides a secure communication channel over the Internet that requires authentication to set up the channel and encrypts all traffic flowing through the channel.

Related Laws, Regulations, or Policies

Hackensack Board of Education

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)
H. 5890 - Access To Education, Student Privacy, and Immigration Enforcement

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; N.J.S.A. 18A:36-19a
G. N.J.S.A. 47:1A-1 et seq.

Federal Legislation and Guidelines

A. Family Educational Rights and Privacy Act of 1974 (FERPA)
B. Protection of Pupil Rights Amendment (PPRA)
C. Children's Online Privacy Protection Rule (COPPA)
D. Health Insurance Portability and Accountability Act of 1996 (HIPAA)
E. Electronic Communications Privacy Act of 1986 (ECPA)
F. NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization
G. NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations
H. NIST Publication 800-60: Guide for Mapping Types of Information and Information Systems to Security Categories

Other Resources

- FERPA FAQ for Parents and Students
- Payment Card Industry Data Security Standard (PCI DSS)

Consequences

Violation of this policy may incur the same types of disciplinary measures and consequences as violations of other District policies, including progressive discipline up to and including termination of employment, or, in the cases where students are involved, reporting of a Student Code of Conduct violation.

Violation of this policy may also result in termination of contracts or commitments to vendors and other affiliates. Legal action may be pursued where appropriate.

Questions/Waivers

The District Technology Coordinator is responsible for this policy. The DTC or designee must approve any exception to this policy or related procedures.

Please address all questions and concerns to privacy@hackensackschools.org.

Appendix I:

Additional Data Privacy and Security Requirements for Third Parties/Vendors

Background:

This appendix serves as an addendum to the data privacy and security requirements and sets specific requirements for third parties (organizations, vendors, etc.) that may utilize, store or transmit District data as either an intermediary or contracted entity or individual.

Scope:

Any third party entities or individuals that collect, store or transmit District data and any associated computer systems, storage devices/media and networks.

Requirements:

In addition to the terms specified in the District's Data Privacy and Security Policy, third party entities/individuals must:

- Identify and assess information security risks regularly and develop/maintain a risk treatment plan to reduce the risk to the confidentiality, integrity and availability of the information it holds or processes.
- Work to reduce or eliminate security incidents
- Minimize the impact of any such incidents
- Continually improve the company's ability to assess, detect, reduce, avoid and ameliorate information security risks and/or incidents
- Work to avoid a negative impact to the District's reputation and brand as a result of any security breach.
- Protect the information of all interested parties including the personal information of its customers.
- Comply with any legal, regulatory or contractual requirements in respect of the data it holds about individuals.
- Follow best practices for data collection and security.
- Seek to continually improve the company's Information Security Management System(s)

- Maintain a Data Security Policy outlining/governing:
    - Types of data collected along with rationale for collection
    - Data collection, storage and usage practices/procedures
    - Data security standards

    - Employee access to data
    - Disclosure/Sharing of District data with any other parties not directly contracted by the District.
    - Policy review
    - Statement regarding how/when changes are made to the policy and how they will be communicated

- Designate a Data Protection Officer that at a minimum is tasked with:
    - Reviewing Data Protection and related policies
    - Advising other staff on Data Protection issues
    - Ensuring that Data Protection induction and training takes place
    - Notification
    - Handling subject access requests
    - Approving unusual or controversial disclosures of personal data
    - Approving contracts with Data Processors

Minimum required Data Security Standards:

- District Data must be encrypted at rest.
- District Data must be encrypted in transit using SSL Encryption.
- All access to District data must be logged and logs maintained for a minimum period of 90 days.
- Access by employees or third parties (excluding District users) to District Data must be protected by multi-factor authentication.
- Remote desktop access to systems that store or handle District data is disabled by default and only enabled on an as-needed basis.
- All data must be stored in an ISO 27001 or equally secure facility in the United States or its territories.
- All data must be backed up regularly and securely.
- Any relevant data security contracts that have been entered into between the vendor/organization/individual and another party must be disclosed to the District.
- In order to comply with relevant legislation:
    - Any data relating to or created by a Student should be deleted if a request to do so is made by a parent of the student. However, the vendor must verify the validity and confirm the authority of the person or persons making the request by contacting the School or District.

- Operate a Business Continuity Plan to deliver continuity of service in the event of a disaster. This plan should cover situations such as:
    - Fire
    - Flash flood
    - Pandemic
    - Power Outage
    - Theft
- All staff who have access to any kind of District data will have their responsibilities outlined during their induction procedures.
- Data Protection will be included in foundation training for all staff.
- Staff are required to sign an electronic form signifying that they have read, understood and accept the Data Security Policy.
- Data security incidents should be classified according to severity:
    - Level 1: Incidents such as unsuccessful exploit attempts that do not involve data loss should be classified as Level 1 - Non Critical Incidents. Level 1 incidents do not require customer notification since there has been no impact to privacy.
    - Level 2: Incidents that do involve data loss (even suspected data loss) will be classified as Level 2 - Critical Incidents and require notification to the District if the District's data may have been impacted.
- Data/Security Policies must be audited at a minimum once per year.
- Penetration and vulnerability testing of all in-scope systems and networks must be conducted at a minimum twice per year and any identified gaps must be communicated to the District along with a remediation plan outlining steps, responsible parties and a target date for resolution.

Appendix II:

Data Classification Examples by Visibility Classification

Note: Common examples are provided below but this table is not intended to be an exhaustive list.

<table>
<tr><th>Data Security Classification</th><th>Examples</th></tr>
<tr><td>Public</td><td>

Employee data
Name
Email address
Photo
Job title(s)
Job description
Education and training
Work location
Work phone number
Honors and awards received
Student Directory information, unless the parent or legal guardian has requested non-disclosure (suppressed)
Name
Address
Email address
Photo
Dates of enrollment/registration
Enrollment/registration status
Grade
School
Class
Academic awards and honors received
Degree received
Student activities/groups
Extra-curricular activities
Course offerings
State-released De-identified/Aggregated Academic Performance Data

</td></tr>
</table>

<table>
<tr><th>Data Security Classification</th><th>Examples</th></tr>
<tr><td></td><td>
Number of Harassment, Intimidation and Bullying (HIB) Claims/Investigations/Findings
User-Friendly Budgets
Donation/Gift information
Requests for Proposals/Bids
Board of Education Meeting Agendas/Public Session Minutes
Press Releases
</td></tr>
<tr><td>Sensitive</td><td>
Employee or Student Data
Birth date/Age
Home phone number (see Student Directory information)
Home address (see Student Directory information)
Government issued ID number (driver's license, passport)
Assigned Parking Space Number
Gender/sexual orientation
Ethnicity
Residency Status
Veteran and disability status

Employee Data
Previous work experience
First and last employment
Terms of buy-out agreements
Employment contract (with confidential items redacted)
Badge number
Work Schedule
Timesheets
Expense reimbursements
Employee ID number
Salary
Gross pension
Value and nature of fringe benefits

Student Directory information if parent or legal guardian has requested non-disclosure (suppressed)
</td></tr>
</table>

<table>
<tr><th>Data Security Classification</th><th>Examples</th></tr>
<tr><td></td><td>

Name
Address
Email address
Telephone number
Dates of enrollment/registration
Enrollment/registration status
School
Class
Academic awards and honors received
Degree received
Student activities/groups

Student Non-Directory data, including

Grades
Courses taken
Class schedule
Test scores (including State and any National Tests)
Guidance records
Educational services received
Disciplinary incidents/actions (including HIB-related claims and incidents)
Attendance Records
Student ID number
Immunization records
Health Services Records

Linking a library patron’s personal identity with materials requested or borrowed by the person or with a specific subject about which the person has requested information or materials
Location of assets (e.g., specific information on where the District physically or electronically stores data, or technology that must be protected)
Passwords/PIN numbers
Biometrics
Invoices and purchase orders
Payroll timesheets

</td></tr>
</table>

Data Security Classification	Examples
	• Vendor contracts • Lease/Rental agreements • Submitted Requests for Proposals/Bids (Opened) • Unpublished academic data that have not been made public, such as de-identified data or research materials
Confidential	• Social security number • Legal investigations conducted by the District • Personnel Records (not mentioned above including Observations and Evaluations) • Bank account information for individuals • Dependent information • Sealed Bids • Board of Education Executive Session Minutes