



# Hackensack Public Schools **Data Privacy and Security Guidelines**

Updated April 2023

## Contents

Purpose .....	3
Scope .....	3
Effective Date.....	3
Policy.....	4
Data Classification Schema .....	4
Data Visibility Classifications.....	4
Data Security Standards.....	6
Contracts with Third Parties.....	14
Roles and Responsibilities .....	14
Collection/Use of District Data.....	15
Sharing/Transfer of District Data .....	15
Approved Third-Party Services .....	15
Training.....	15
Reporting Incidents .....	15
Related Laws, Regulations, or Policies.....	17
Consequences .....	18
Questions/Waivers .....	19
Appendix I: Additional Data Requirements for Third Parties/Vendors .....	20
Appendix II: Data Classification Examples by Visibility Classification .....	23
Appendix III: Confidentiality Agreement for District Employees.....	27
Data Sharing Request Form.....	28

## **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. Data security requirements for Proprietary Data are determined by the contracting agency and are therefore not included in this guide.

## **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.

## 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. Directory information for students, faculty, and staff who have requested non-disclosure (e.g., per FERPA for students.)
  4. 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. Disabilities or Medical Conditions
  3. Disciplinary Records
  4. Student Academic Records
  5. Residency status
  6. Personnel records (e.g., evaluations, letters of reprimand, etc.)
  7. Security Information (i.e., School Security Plans, camera locations, recordings, Drill schedules, etc.)
  8. Authentication tokens (e.g., personal digital certificates, passwords, pin numbers, biometric data)
- D. **Proprietary Data** - Confidential or copyrighted data that may include, but is not limited to, trade secrets, print and digital content, processes and procedures owned by a third-party contractor or service provider.

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

## Data Security Standards

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	Sensitive	Confidential
Access Controls	<ul style="list-style-type: none"> <li>• No restriction for viewing.</li> <li>• Authorization by Data Steward or designee required for modification; supervisor approval also required if not a self-service function.</li> </ul>	<ul style="list-style-type: none"> <li>• Viewing and modification restricted to authorized individuals as needed for business-related roles.</li> <li>• While individual user accounts are highly recommended, shared accounts may be permitted on a case-by-case basis.</li> <li>• Data Steward or designee grants permission for access, plus approval from supervisor.</li> <li>• Authentication and authorization required for access.</li> <li>• <b>Multi-factor authentication highly recommended.</b></li> </ul>	<ul style="list-style-type: none"> <li>• Viewing and modification restricted to authorized individuals as needed for business-related roles.</li> <li>• Sharing of accounts not permitted.</li> <li>• Data Steward or designee grants permission for access, plus approval from supervisor.</li> <li>• <b>Multi-factor Authentication</b> and authorization required for access.</li> <li>• <b>Cannot be accessed/viewed on personal devices unless devices meet district security controls (i.e. antivirus, screen lock, idle timeout, etc.).</b></li> <li>• Confidentiality agreement required.</li> </ul>

Security Control Category	Data Classification		
	Public	Sensitive	Confidential
Copying/Printing (applies to both paper and electronic forms)	<ul style="list-style-type: none"> <li>No restrictions.</li> </ul>	<ul style="list-style-type: none"> <li>Data should only be printed when there is a legitimate need.</li> <li>Copies must be limited to individuals with a need to know.</li> <li>Data should not be left unattended on a printer.</li> </ul>	<ul style="list-style-type: none"> <li>Data should only be printed when there is a legitimate need.</li> <li>Copies must be limited to individuals authorized to access the data and have signed a confidentiality agreement.</li> <li>Data should not be left unattended on a printer.</li> <li>Copies should be labeled "Confidential" when possible.</li> </ul>

Security Control Category	Data Classification		
	Public	Sensitive	Confidential
Network Security	<ul style="list-style-type: none"> <li>• May reside on a public network.</li> <li>• Protection with a firewall recommended.</li> <li>• IDS/IPS protection recommended.</li> <li>• Protection only with router ACLs acceptable.</li> </ul>	<ul style="list-style-type: none"> <li>• Protection with a network firewall required.</li> <li>• IDS/IPS protection required.</li> <li>• Protection with router ACLs optional.</li> <li>• Servers hosting the data should not be visible to entire Internet.</li> <li>• 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.</li> <li>• May be in a shared network server subnet with a common firewall ruleset for the set of servers.</li> </ul>	<ul style="list-style-type: none"> <li>• Protection with a network firewall using "default deny" ruleset required.</li> <li>• IDS/IPS protection required.</li> <li>• Protection with router ACLs optional.</li> <li>• Servers hosting the data cannot be visible to the entire Internet, nor to unprotected subnets and guest wireless networks.</li> <li>• Must have a firewall ruleset dedicated to the system.</li> <li>• The firewall ruleset should be reviewed periodically.</li> <li>• 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.</li> </ul>



Security Control Category	Data Classification		
	Public	Sensitive	Confidential
System Security	<ul style="list-style-type: none"> <li>• Must follow general best practices for system management and security.</li> <li>• Host-based software firewall recommended.</li> </ul>	<ul style="list-style-type: none"> <li>• Must follow District-specific and OS-specific best practices for system management and security.</li> <li>• Host-based software firewall required.</li> <li>• Host-based software IDS/IPS recommended</li> <li>• 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.</li> </ul>	<ul style="list-style-type: none"> <li>• Must follow District-specific and OS-specific best practices for system management and security.</li> <li>• Host-based software firewall required.</li> <li>• Host-based software IDS/IPS recommended.</li> <li>• 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.</li> <li>• Mobile Devices: Multi-Factor Authentication required.</li> </ul>
Virtual Environments	<ul style="list-style-type: none"> <li>• May be hosted in a virtual server environment.</li> <li>• All other security controls apply to both the host and the guest virtual machines.</li> </ul>	<ul style="list-style-type: none"> <li>• May be hosted in a virtual server environment.</li> <li>• All other security controls apply to both the host and the guest virtual machines.</li> <li>• Should not share the same virtual host environment with guest virtual servers of other security classifications.</li> </ul>	<ul style="list-style-type: none"> <li>• May be hosted in a virtual server environment.</li> <li>• All other security controls apply to both the host and the guest virtual machines.</li> <li>• Cannot share the same virtual host environment with guest virtual servers of other security classifications.</li> </ul>

Security Control Category	Data Classification		
	Public	Sensitive	Confidential
Physical Security	<ul style="list-style-type: none"> <li>• System must be locked or logged out when unattended.</li> <li>• Host-based software firewall recommended.</li> </ul>	<ul style="list-style-type: none"> <li>• System must be locked or logged out when unattended.</li> <li>• Hosted in a secure location required; a Secure Data Center is recommended.</li> </ul>	<ul style="list-style-type: none"> <li>• System must be locked or logged out when unattended.</li> <li>• Hosted in a Secure Data Center required.</li> <li>• Physical access must be monitored, logged, and limited to authorized individuals 24x7.</li> </ul>
Remote Access to systems hosting the data	<ul style="list-style-type: none"> <li>• No restrictions.</li> </ul>	<ul style="list-style-type: none"> <li>• Access restricted to local network or general District Virtual Private Network (VPN) service.</li> <li>• Remote access by third party for technical support limited to authenticated, temporary access via secure protocols.</li> </ul>	<ul style="list-style-type: none"> <li>• Restricted to local network or secure VPN group.</li> <li>• Unsupervised remote access by third party for technical support not allowed.</li> <li>• Multi-factor authentication required.</li> </ul>
Data Storage	<ul style="list-style-type: none"> <li>• Storage on a secure server recommended.</li> <li>• Storage in a secure Data Center recommended.</li> <li>• Storage on District-approved “cloud-based” applications permitted.</li> </ul>	<ul style="list-style-type: none"> <li>• Storage on a secure server recommended.</li> <li>• Storage in a secure Data Center recommended.</li> <li>• <b>Storage on portable storage not permitted. (i.e., USB drives).</b></li> <li>• <b>Temporary storage permitted on individual’s district provided</b></li> </ul>	<ul style="list-style-type: none"> <li>• Storage on a secure server required.</li> <li>• Storage in Secure Data Center required.</li> <li>• <b>Should not be stored on an individual’s workstation or mobile device (e.g., a laptop computer, smartphone); if stored on a mobile device, must use</b></li> </ul>

Security Control Category	Data Classification		
	Public	Sensitive	Confidential
		<p>workstation or mobile device (excluding personal and shared devices). Should be destroyed/deleted once no longer needed.</p> <ul style="list-style-type: none"> <li>• If stored on individual's mobile device, multi-factor authentication highly recommended.</li> <li>• Data encryption recommended.</li> <li>• Storage on District-approved "cloud-based" applications permitted (<b>i.e., District Google Drive</b>)(Multi-factor authentication highly recommended).</li> </ul>	<p>whole-disk encryption and multi-factor authentication for initial login. Data must be destroyed/deleted once no longer needed.</p> <ul style="list-style-type: none"> <li>• Storage on a personal device or portable storage <b><u>strictly prohibited</u></b>.</li> <li>• Encryption on backup media required.</li> <li>• AES Encryption required with 256-bit or longer key.</li> <li>• Paper/hard copy: do not leave unattended where others may see it; store in a secure location.</li> <li>• Storage on District-approved "cloud-based" applications permitted (<b>i.e., District Google Drive</b>)(Multi-factor authentication required).</li> <li>• Storage on non-District approved "cloud-based" applications <b><u>strictly prohibited</u></b>.</li> </ul>

Security Control Category	Data Classification		
	Public	Sensitive	Confidential
Transmission	<ul style="list-style-type: none"> <li>No restrictions.</li> </ul>	<ul style="list-style-type: none"> <li>Encryption highly recommended (e.g., via SSL or secure file transfer protocols).</li> </ul>	<ul style="list-style-type: none"> <li>Encryption required (e.g., via SSL or secure file transfer protocols).</li> <li>Cannot transmit via e-mail unless encrypted and secured with a digital signature.</li> </ul>
Backup/Disaster Recovery	<ul style="list-style-type: none"> <li>Backups required; daily backups recommended.</li> </ul>	<ul style="list-style-type: none"> <li>Daily backups required.</li> <li>Off-site storage recommended.</li> </ul>	<ul style="list-style-type: none"> <li>Daily backups required.</li> <li>Off-site storage in a secure location required.</li> <li>Air-gapped backups required for critical systems/data.</li> </ul>
Media Sanitization and Disposal (hard drives, CDs, DVDs, tapes, paper, etc.)	<ul style="list-style-type: none"> <li>Please see “<a href="#">Best Practices for Data Destruction</a>” from the Privacy Technical Assistance Center as well as the <a href="#">NIST Special Publication 800-88 Guidelines for Media Sanitization</a>.</li> <li>Paper: no restrictions.</li> </ul>	<ul style="list-style-type: none"> <li>Please see “<a href="#">Best Practices for Data Destruction</a>” from the Privacy Technical Assistance Center as well as the <a href="#">NIST Special Publication 800-88 Guidelines for Media Sanitization</a>.</li> </ul>	<ul style="list-style-type: none"> <li>Please see “<a href="#">Best Practices for Data Destruction</a>” from the Privacy Technical Assistance Center as well as the <a href="#">NIST Special Publication 800-88 Guidelines for Media Sanitization</a>.</li> </ul>

Security Control Category	Data Classification		
	Public	Sensitive	Confidential
Training	<ul style="list-style-type: none"> <li>General security awareness training recommended.</li> <li>System administration training recommended.</li> </ul>	<ul style="list-style-type: none"> <li>General security awareness training required.</li> <li>System administration training required.</li> <li>All employees must pass criminal background check in accordance with State law.</li> <li>Data security training required.</li> </ul>	<ul style="list-style-type: none"> <li>General security awareness training required.</li> <li>System administration training required.</li> <li>All employees must pass criminal background check in accordance with State law.</li> <li>Data security training required.</li> <li>Applicable policy and regulation training required.</li> <li>Confidentiality Agreement Required.</li> </ul>
Audit Schedule	<ul style="list-style-type: none"> <li>As needed</li> </ul>	<ul style="list-style-type: none"> <li>As needed</li> </ul>	<ul style="list-style-type: none"> <li>Twice per year</li> </ul>
Incident Reporting	None	<ul style="list-style-type: none"> <li>Report to District Technology Coordinator.</li> </ul>	<ul style="list-style-type: none"> <li>Report to building administrator/supervisor and District Technology Coordinator immediately.</li> </ul>
Breach Response	<ul style="list-style-type: none"> <li>Notification: None required.</li> </ul>	<ul style="list-style-type: none"> <li>Follow "<a href="#"><u>Hackensack Public Schools Information Security Incident Response Guide</u></a>"</li> </ul>	<ul style="list-style-type: none"> <li>Follow "<a href="#"><u>Hackensack Public Schools Information Security Incident Response Guide</u></a>"</li> </ul>

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. **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. **Sensitive/Confidential Data cannot not be shared externally without approval. This includes sharing data with outside individuals, agencies and Third-Party service providers/vendors (unless service/vendor was previously approved and data being shared meets the approved purpose).**

## 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

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 receive a copy of this policy along with all applicable District Acceptable Use policies (2360-2361) and acknowledge 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.

## Reporting Incidents

In order to ensure compliance with New Jersey law, which requires all public agencies to report all “cybersecurity incidents,” suspected and/or confirmed violations of the Data Privacy Standards set forth in this document must be reported as soon as possible to the District Incident Response Team at [ir@hackensackschools.org](mailto:ir@hackensackschools.org), who will determine next steps in accordance with the District’s Incident Response Plan.

## 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.

**Cybersecurity Incident** - means a malicious or suspicious event occurring on or conducted through a computer network that jeopardizes the integrity, confidentiality, or availability of an information system or the information the system processes, stores, or transmits.

**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.  
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).

**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.

**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](mailto:privacy@hackensackschools.org).

# Appendix I:

## Additional Data 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.

### Definitions:

**“District Data”** refers to any information, data, records, files, or content, whether in digital or physical form, that is collected, processed, stored, generated or managed by the employees, students and contractors of the Hackensack Board of Education. This includes but is not limited to student records, educational materials, employee information, financial records, and any other data associated with the operations and activities of the Hackensack Board of Education. District Data encompasses both personal and non-personal information and is subject to the privacy and security provisions outlined in this District’s Data Privacy and Security Policy.

### Expectations:

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

- Proactively identify and address information security risks that may impact the confidentiality, integrity and availability of the customer information it holds or processes as part of a documented information security/risk management process.
- Continually improve the company’s ability to assess, detect, reduce, avoid and remediate information security risks and/or incidents.
- Work to avoid a negative impact to the District’s reputation and brand as well as that of its stakeholders as a result of any security incident/breach.
- Comply with any applicable legal, regulatory or contractual requirements in respect to the confidential or protected data it holds about individuals (i.e., FERPA, COPPA, PPRA, HIPAA).
- Follow industry best practices for data collection, storage and security and secure coding (if applicable).
- Maintain a Data Security Policy outlining/governing, at a minimum:
  - 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/Customer
- Policy review
- Statement regarding how/when changes are made to the policy and how they will be communicated.
- Designate a Data Protection/Information Security Officer that, at a minimum, is tasked with:
  - Reviewing Data Protection/Security and related policies
  - Advising other staff on Data Security issues
  - Ensuring that Data Security induction and training takes place
  - Notification to stakeholders regarding data security-related developments
  - Handling subject access requests
  - Reviewing/Approving unusual or controversial disclosures of personal data
  - Reviewing/Approving contracts with Data Processors

#### **Minimum required Data Security Standards:**

1. Encrypt District Data at-rest and in-transit using industry-standard encryption protocols such as AES-256 for data at-rest and TLS 1.2 or higher for data in-transit.
2. Maintain access logs for a minimum of 90 days, conducting periodic reviews to identify and investigate any suspicious activity.
3. Multi-Factor Authentication:
  - a. Enforce multi-factor authentication for all employees and third parties accessing District Data (excluding district users).
  - b. Provide multi-factor authentication for district users with access to confidential/sensitive information, where applicable.
4. Store all district data in a facility compliant with ISO 27001 or NIST 800-53 standards, or an equivalent level of security, located in the United States or its territories.
5. Conduct regular, automated backups of district data daily, storing them securely offsite within the United States or its territories.
6. Maintain and regularly test a documented data recovery plan to ensure timely restoration in case of data loss or system failures.
7. Disclose any agreements granting access to district data between the vendor and third parties to the District.
8. Delete any data related to or created by a student upon request by a parent, verifying the request's validity by contacting the School or District.
9. Establish and maintain comprehensive Disaster Recovery and Business Continuity Plans to ensure continuous services during fire, flash floods, pandemics, power outages, theft, and cyberattacks.
10. Employee Training/Compliance:
  - a. Clearly outline responsibilities for all staff with access to District data during their induction procedures.

- b. Include Data Protection in foundational training for all staff.
  - c. Ensure staff sign an electronic form indicating their understanding and acceptance of the organization's Data Security Policy.
- 11. Classify data security incidents based on severity.
  - a. Level 1: Classify unsuccessful exploit attempts as Level 1 - Non-Critical Incidents.
  - b. Level 2: Classify incidents involving data loss as Level 2 - Critical Incidents, requiring notification to the District.
- 12. Conduct annual reviews and audits of Data/Security Policies to ensure ongoing effectiveness and compliance.
- 13. Perform annual penetration and vulnerability testing on all in-scope systems and networks.
  - a. Address identified gaps within a reasonable timeframe, considering severity and exploitability of risks.
  - b. Share non-specific/generalized information on identified gaps, including relevant vulnerability/risk scoring, and expected timeframes for resolution with the District within ten (10) business days.

# 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.

Data Security Classification	Examples
Public	<ul style="list-style-type: none"> <li>• Employee data <ul style="list-style-type: none"> <li>○ Name</li> <li>○ Email address</li> <li>○ Photo</li> <li>○ Job title(s)</li> <li>○ Job description</li> <li>○ Education and training</li> <li>○ Work location</li> <li>○ Work phone number</li> <li>○ Honors and awards received</li> </ul> </li> <li>• Student Directory information, unless the parent or legal guardian has requested non-disclosure (suppressed) <ul style="list-style-type: none"> <li>○ Name</li> <li>○ Address</li> <li>○ Email address</li> <li>○ Photo</li> <li>○ Dates of enrollment/registration</li> <li>○ Enrollment/registration status</li> <li>○ Grade</li> <li>○ School</li> <li>○ Class</li> <li>○ Academic awards and honors received</li> <li>○ Degree received</li> <li>○ Student activities/groups</li> <li>○ Extra-curricular activities</li> </ul> </li> <li>• Course offerings</li> <li>• State-released De-identified/Aggregated Academic Performance Data</li> </ul>

Data Security Classification	Examples
	<ul style="list-style-type: none"> <li>• Number of Harassment, Intimidation and Bullying (HIB) Claims/Investigations/Findings</li> <li>• User-Friendly Budgets</li> <li>• Donation/Gift information</li> <li>• Requests for Proposals/Bids</li> <li>• Board of Education Meeting Agendas/Public Session Minutes</li> <li>• Press Releases</li> </ul>
<b>Sensitive</b>	<ul style="list-style-type: none"> <li>• Employee or Student Data <ul style="list-style-type: none"> <li>○ Birth date/Age</li> <li>○ Home phone number (see Student Directory information)</li> <li>○ Home address (see Student Directory information)</li> <li>○ Government issued ID number (driver's license, passport)</li> <li>○ Assigned Parking Space Number</li> <li>○ Gender/sexual orientation</li> <li>○ Ethnicity</li> <li>○ Veteran and disability status</li> </ul> </li> <li>• Employee Data <ul style="list-style-type: none"> <li>○ Previous work experience</li> <li>○ First and last employment</li> <li>○ Terms of buy-out agreements</li> <li>○ Employment contract (with confidential items redacted)</li> <li>○ Badge number</li> <li>○ Work Schedule</li> <li>○ Timesheets</li> <li>○ Expense reimbursements</li> <li>○ Employee ID number</li> <li>○ Salary</li> <li>○ Gross pension</li> <li>○ Value and nature of fringe benefits</li> </ul> </li> <li>• Student Directory information if parent or legal guardian has requested non-disclosure (suppressed) <ul style="list-style-type: none"> <li>○ Name</li> </ul> </li> </ul>



Data Security Classification	Examples
	<ul style="list-style-type: none"> <li>○ Address</li> <li>○ Email address</li> <li>○ Telephone number</li> <li>○ Dates of enrollment/registration</li> <li>○ Enrollment/registration status</li> <li>○ School</li> <li>○ Class</li> <li>○ Academic awards and honors received</li> <li>○ Degree received</li> <li>○ Student activities/groups</li> <li>• Student Non-Directory data, including <ul style="list-style-type: none"> <li>○ Grades</li> <li>○ Courses taken</li> <li>○ Class schedule</li> <li>○ Test scores (including State and any National Tests)</li> <li>○ Guidance records</li> <li>○ Educational services received</li> <li>○ Disciplinary incidents/actions (including HIB-related claims and incidents)</li> <li>○ Attendance Records</li> <li>○ Student ID number</li> <li>○ Immunization records</li> <li>○ Health Services Records</li> </ul> </li> <li>• 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</li> <li>• Location of assets (e.g., specific information on where the District physically or electronically stores data, or technology that must be protected)</li> <li>• Passwords/PIN numbers</li> <li>• Biometrics</li> <li>• Invoices and purchase orders</li> <li>• Payroll timesheets</li> <li>• Vendor contracts</li> </ul>

<b>Data Security Classification</b>	<b>Examples</b>
	<ul style="list-style-type: none"> <li>• Lease/Rental agreements</li> <li>• Submitted Requests for Proposals/Bids (Opened)</li> <li>• Unpublished academic data that have not been made public, such as de-identified data or research materials</li> </ul>
<b>Confidential</b>	<ul style="list-style-type: none"> <li>• Social security number</li> <li>• Residency Status</li> <li>• Legal investigations conducted by the District</li> <li>• Personnel Records (not mentioned above including Observations and Evaluations)</li> <li>• Bank account information for individuals</li> <li>• Dependent information</li> <li>• Sealed Bids</li> <li>• Board of Education Executive Session Minutes</li> </ul>

# Appendix III:

## Confidentiality Agreement for District Employees

As a Hackensack Public Schools employee, I understand that I may have access to confidential information about students and/or employees in the course of my job responsibilities. I recognize the importance of maintaining the confidentiality of this information to protect the privacy and rights of individuals and the school district and to comply with all applicable federal and state laws.

Therefore, I agree to the following:

1. I will only access confidential information that is necessary for the performance of my job duties.
2. I will not disclose confidential information to anyone who is not authorized to receive it, including family members and friends.
3. I will take reasonable steps to safeguard confidential information against unauthorized access, disclosure, or misuse.
4. I will not use confidential information for personal gain or any other unauthorized purpose.
5. I will report any suspected unauthorized access, disclosure, or misuse of confidential information to my supervisor or designated school official immediately.
6. I will abide by the security guidelines set forth in the Hackensack Public Schools District Data Privacy and Security Guidelines and by all applicable state and federal laws
7. I understand that any breach of this confidentiality agreement may result in disciplinary action, up to and including termination of employment.

I acknowledge that I have read and understand this confidentiality agreement and agree to comply with its terms and conditions.

---

Signed

---

Print Name

---

Date

# Data Sharing Request Form

Department/Employee Information					
Employee Name:				Department/School	
Email:			Phone:		
Purpose of Data Sharing					
Please describe the purpose of the data sharing:					
What data will be shared?					
Include specific data sets or submit any relevant guides indicating necessary data fields/columns. Use next page to specify fields.					
Personnel <input type="checkbox"/> Student Demographics <input type="checkbox"/> Student Educational Records <input type="checkbox"/> Photos <input type="checkbox"/> Budget/Financial: <input type="checkbox"/> Payroll <input type="checkbox"/> Contracts/Bids <input type="checkbox"/> Other (specify): _____					
Recipient Information					
Organization/Agency (if any):					
Contact Name:			Email:		
Phone:					
Mailing Address:					
Data Security					
How will the data be transmitted? <small>(e.g. encrypted email, secure file transfer)</small>				Frequency <small>(e.g. weekly, monthly, once)</small>	
Will the data be de-identified or anonymized before sharing?				<input type="checkbox"/> Yes <input type="checkbox"/> No	
How will the data be stored and secured by the recipient organization/agency?					
Please attach/submit any relevant Data Policies, including Terms of Use and Privacy Policy.					
Will the recipient organization/agency be allowed to share this data with other organizations or individuals (aside from employees/contractors)?				<input type="checkbox"/> Yes <input type="checkbox"/> No	
Data Use Agreement					
Will a Data Use Agreement be established between the district and the recipient organization/agency?				<input type="checkbox"/> Yes <input type="checkbox"/> No	
If so, has the Data Use Agreement been reviewed and approved by the district's legal counsel or Board of Education?				<input type="checkbox"/> Yes <input type="checkbox"/> No	
Approval					
Employee Signature				Supervisor Signature	
Employee Printed Name				Supervisor Printed Name	
For District Use Only					
Date Received:		Reviewed By:		Approved/Rejected	<input type="checkbox"/> Yes <input type="checkbox"/> No
Comments:					

## Data Fields

	Data Field	System (if known)	Description/Notes
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			