



# HOBOKEN BOARD OF EDUCATION

OFFICE OF THE SUPERINTENDENT OF SCHOOLS

158 Fourth Street ❖ Hoboken, NJ 07030 ❖ 201.356.3601 ❖ Fax: 201.356.3641

Dr. Christine A. Johnson  
Superintendent of Schools  
[Christine.Johnson@hoboken.k12.nj.us](mailto:Christine.Johnson@hoboken.k12.nj.us)

## Data Governance Plan

### Data Governance Framework

HPSD has a three-tiered data governance framework to ensure that data is protected at all levels of Hoboken's educational system.

Three-Tiered Data Governance Framework		
Tier I	Executive Steering Committee	Superintendent of Schools Chief Technology Officer Business Administrator
Tier II	Data Governance Team	Assistant Superintendent All Principals and Vice Principals District Data Manager Lead Technician
Tier III	Data Stewards	Staff with data access

Furthermore, this HPSP Data Governance Plan

- Designates the HPSP as the steward for all confidential information maintained within the HPSP
- Designates Data Stewards access for all confidential information.
- Requires Data Stewards to maintain a record of all confidential information that they are responsible for.
- Requires Data Stewards to manage confidential information according to this policy and all other applicable policies, standards and plans.
- Complies with all legal, regulatory, and contractual obligations regarding privacy of agency data. Where such requirements exceed the specific stipulation of this policy, the legal, regulatory, or contractual obligation shall take precedence.
- Provides the authority to design, implement, and maintain privacy procedures meeting HPSP standards concerning the privacy of data in motion, at rest and processed by related information systems.
- Ensures that all HPSP board members, employees, contractors, and volunteers comply with the policy and undergo annual privacy training.
- Provides policies and process for
  - Systems administration,

Where Students Come First

- Network security,
- Application security,
- Endpoint, server, and device security,
- Identity, authentication, and access management,
- Data protection and cryptography,
- Monitoring, vulnerability, and patch management,
- High availability, disaster recovery, and physical protection,
- Incident Responses,
- Acquisition and asset management, and
- Policy, audit, e-discovery, and training.

## **Individual Responsibilities**

The following outlines individual HPSD responsibilities.

### **District Data Manager Responsibilities**

1. Authorize and manage the sharing, outside of the education entity, of personally identifiable student data from a cumulative record for the education entity.
2. Act as the primary local point of contact for the state student data officer.
3. Ensure that personally identifiable student data that are shared meet the following criteria:
  - of a student with the student and the student's parent
  - required by state or federal law
  - in an aggregate form with appropriate data redaction techniques applied
  - for a school official
  - for an authorized caseworker or other representative of the Department of Human Services or the Juvenile Court
  - in response to a subpoena issued by a court.
  - directory information
  - submitted data requests from external researchers or evaluators,
4. Prevent or refrain from sharing personally identifiable student data for the purpose of external research or evaluation.
5. Create and maintain a list of all District staff that have access to personally identifiable student data.
6. Ensure annual District level training on data privacy to all staff members, including volunteers. Document all staff names, roles, and training dates, times, locations, and agendas.

### **IT Systems Security Manager Responsibilities**

1. Acts as the primary point of contact for state student data security administration in assisting the board to administer this part;

2. Ensures compliance with security systems laws throughout the public education system, including:
  - providing training and support to applicable HPSD employees; and
  - producing resource material, model plans, and model forms for District systems security;
3. Investigates complaints of alleged violations of systems breaches;
4. Provides an annual report to the board on HPSD's systems security needs.

### **Employee Non-Disclosure Assurance**

Employee non-disclosure assurances are intended to minimize the risk of human error and misuse of information.

#### Scope

All HPSD board members, employees, contractors and volunteers must sign and obey the HPSD Employee Non-Disclosure Agreement (See Appendix A), which describes the permissible uses of state technology and information

#### Non-Compliance

Non-compliance with the agreements shall result in consequences up to and including removal of access to HPSD network; if this access is required for employment, employees and contractors may be subject to dismissal.

#### Non-Disclosure Assurances

All student data utilized by HPSD is protected as defined by the Family Educational Rights and Privacy Act (FERPA) and NJ statute. This policy outlines the way HPSD staff is to utilize data and protect personally identifiable and confidential information. A signed agreement form is required from all HPSD staff to verify agreement to adhere to/abide by these practices and will be maintained in HPSD Human Resources. All HPSD employees (including contract or temporary) will:

1. Complete a Security and Privacy Fundamentals Training.
2. Complete a Security and Privacy Training for Researchers and Evaluators, if your position is a research analyst or if requested by the District Data Manager.
3. Consult with HPSD internal data owners when creating or disseminating reports containing data.
4. Use password-protected state-authorized computers when accessing any student-level or staff-level records.
5. NOT share individual passwords for personal computers or data systems with anyone.
6. Log out of any data system/portal and close the browser after each use.

7. Store sensitive data on appropriate-secured location. Unsecured access and flash drives, DVD, CD-ROM or other removable media, or personally owned computers or devices are not deemed appropriate for storage of sensitive, confidential or student data.
8. Keep printed reports with personally identifiable information in a locked location while unattended, and use the secure document destruction service provided at HPSD when disposing of such records.
9. NOT share personally identifying data during public presentations, webinars, etc. If users need to demonstrate child/staff level data, demo records should be used for such presentations.
10. Redact any personally identifiable information when sharing sample reports with general audiences, in accordance with guidance provided by the student data manager.
11. Take steps to avoid disclosure of personally identifiable information in reports, such as aggregating, data suppression, rounding, recoding, blurring, perturbation, etc.
12. Delete files containing sensitive data after using them on computers, or move them to secured servers or personal folders accessible only by authorized parties.
13. NOT use email to send screenshots, text, or attachments that contain personally identifiable or other sensitive information. If users receive an email containing such information, they will delete the screenshots/text when forwarding or replying to these messages. If there is any doubt about the sensitivity of the data the Student Data Privacy Manager should be consulted.
14. Use secure methods when sharing or transmitting sensitive data. Sharing within secured server folders is appropriate for HPSD internal file transfer.
15. NOT transmit child/staff-level data externally unless expressly authorized in writing by the data owner and then only transmit data via approved methods.
16. Limit use of individual data to the purposes which have been authorized within the scope of job responsibilities.

## **Data Security and Privacy Training**

### **Purpose**

HPSD will provide a range of training opportunities for all HPSD staff, including volunteers, contractors and temporary employees with access to student educational data or confidential educator records in order to minimize the risk of human error and misuse of information.

### **Scope**

All HPSD board members, employees, and contracted partners.

### **Compliance**

New employees that do not comply may not be able to use HPSD networks or technology.

## Policy

1. Within the first week of employment, all HPSD board members, employees, and contracted partners must sign and follow the HPSD Employee Acceptable Use Policy, which describes the permissible uses of state technology and information.
2. New employees that do not comply may not be able to use HPSD networks or technology. Within the first week of employment, all HPSD board members, employees, and contracted partners also must sign and obey the HPSD Employee Non-Disclosure Agreement, which describes appropriate uses and the safeguarding of student and educator data.
3. All current HPSD board members, employees, and contracted partners are required to participate in an annual Security and Privacy Fundamentals Training Curriculum within 60 days of the adoption of this rule.
4. HPSD requires a targeted Security and Privacy Training for Data Stewards and IT staff for other specific groups within the agency that collect, store, or disclose data. The District Data Manager will identify these groups. District Data Manager will determine the annual training topics for these targeted groups based on HPSD training needs.
5. Participation in the training as well as a signed copy of the Employee Non-Disclosure Agreement will be annually monitored by supervisors. Supervisors and the board secretary will annually report all HPSD board members, employees, and contracted partners who do not have these requirements completed to the Chief Technology Officer.

## Data Disclosure

### Purpose

Providing data to persons and entities outside of the HPSD increases transparency, promotes education in NJ, and increases knowledge about NJ public education. This policy establishes the protocols and procedures for sharing data maintained by the HPSD. It is intended to be consistent with the disclosure provisions of the federal Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g, 34 CFR Part 99

### Policy For Disclosure of Personally Identifiable Information (PII)

#### Student or Student's Parent/Guardian Access

In accordance with FERPA regulations 20 U.S.C. § 1232g (a)(1) (A) (B) (C) and (D), the HPSD will provide parents with access to their child's education records, or an eligible student access to his or her own education records (excluding information on other students, the financial records of parents, and confidential letters of recommendation if the student has waived the right to access), within 45 days of receiving an official request. HPSD is not required to provide data that it does not maintain, nor is HPSD required to create education records in response to an eligible student's request.

#### Third Party Vendor

Third party vendors may have access to students' personally identifiable information if the vendor is designated as a "school official" as defined in FERPA, 34 CFR §§ 99.31(a)(1) and 99.7(a)(3)(iii). A school official may include parties such as: professors, instructors, administrators, health staff, counselors, attorneys, clerical staff, trustees, members of committees and disciplinary boards, and a contractor, consultant, volunteer or other party to whom the school has outsourced institutional services or functions.

All third-party vendors contracting with HPSD must be compliant with New Jersey's law. Vendors determined not to be compliant may not be allowed to enter into future contracts with HPSD without third-party verification that they are compliant with federal and state law, and board rule.

#### Internal Partner Requests

Internal partners to HPSD include any school officials that are determined to have a legitimate educational interest in the information. All requests shall be documented in HPSD's data request ticketing system

#### Governmental Agency Requests

HPSD may not disclose personally identifiable information of students to external persons or organizations to conduct research or evaluation that is not directly related to a state or federal program reporting requirement, audit, or evaluation. The requesting governmental agency must provide evidence the federal or state requirements to share data in order to satisfy FERPA disclosure exceptions to data without consent in the case of a federal or state reporting requirement

- a. audit
- b. evaluation

The District Data Manager will ensure the proper data disclosure avoidance are included if necessary. An Interagency Agreement must be reviewed by legal staff and must include "FERPA-Student Level Data Protection Standard Terms and Conditions or Required Attachment Language."

#### Policy for External Disclosure of Non-Personally Identifiable Information (PII)

##### Scope

External data requests from individuals or organizations that are not intending on conducting external research or are not fulfilling a state or federal reporting requirement, audit, or evaluation.

##### Student Data Disclosure Risk Levels

HPSD has determined two levels of data requests with corresponding policies and procedures for appropriately protecting data based on risk: Low and High. The District

Data Manager will make final determinations on classification of student data requests risk level.

### Low-Risk Data Request Process

Definition: Low-level aggregate data

Examples:

- Graduation rate by year for the state
- Percent of third-graders scoring proficient on a state-mandated ELA assessment

Process: Staff member initiates request of District Data Manager. Data Request forwarded to appropriate Data Steward. Data Steward fulfills request and saves the dataset in a secure folder managed by the District Data Manager. The Data Steward closes the ticket.

### High-Risk Data Request Process

Definition: High-level aggregate data

Examples:

- Social security numbers
- Confidential data as relates to IEP status

Process: Requester creates a ticket, Data Request forwarded to District Data Manager for review. If the request is approved, an MOA is drafted and sent to legal, placed on the board consent calendar, reviewed by the Superintendent, sent to the Purchasing/Contract Manager, sent to District Data Manager, appropriate Data Steward fulfills request, de-identifies data as appropriate, and sends to another Data Steward for Quality Assurance (ensuring student data protection). If it passes QA, data are sent to requester and saves the dataset in a secure folder managed by the District Data Manager. The Data Steward closes the ticket. If it does not pass QA, the data are sent back to the Data Steward for modification.

### Data Disclosure to a Requesting External Researcher or Evaluator

Responsibility: The District Data Manager will ensure the proper data are shared with external researcher or evaluator to comply with federal, state, and board rules.

HPSD may not disclose personally identifiable information of students to external persons or organizations to conduct research or evaluation that is not directly related to a state or federal program audit or evaluation. Data that do not disclose PII may be shared with external researcher or evaluators for projects unrelated to federal or state requirements if:

1. A HPSD Director, Superintendent, or board member sponsors an external researcher or evaluator request.

2. Student data are not PII and are de-identified through disclosure avoidance techniques and other pertinent techniques as determined by the District Data Manager.
3. Researchers and evaluators supply the HPSD a copy of any publication or presentation that uses HPSD data 10 business days prior to any publication or presentation.

## **Data Breach Plan**

### Purpose

Managing data breaches is important to protect the personal data of our students and staff when a data breach occurs. Establishing a plan for responding to a data breach, complete with clearly defined roles and responsibilities, will promote better response coordination and help educational organizations shorten their incident response time. Prompt response is essential for minimizing the risk of any further data loss and, therefore, plays an important role in mitigating any negative consequences of the breach, including potential harm to affected individuals.

### Policy

A data breach generally refers to the unauthorized access and retrieval of information that may include student and staff personal data. HPSD shall follow the steps below to protect information and data.

Concerns about security breaches must be reported immediately to the Lead District Technician who will collaborate with appropriate members of the HPSD executive team to determine whether a security breach has occurred. If the HPSD data breach response team determines that one or more employees or contracted partners have substantially failed to comply with HPSD's Operational Best Practices and Security Policy and relevant privacy policies, they will identify appropriate consequences, which may include termination of employment or a contract and further legal action. Concerns about security breaches that involve the Lead District Technician must be reported immediately to the Superintendent.

If a data breach is detected, the CTO or designee will notify individuals whose personal data may have been compromised. The CTO will notify other third parties such as the police, where relevant. The CTO or designee will notify affected individuals immediately if a data breach involves sensitive personal data. Notifications will be simple to understand, specific and provide clear instructions on what individuals can do to protect themselves. The notification will state how and when the data breach occurred, types of personal data involved in the data breach, and what has been done in response to the risks.

## **Record Retention and Expungement**

### Purpose



Records retention and expungement policies promote efficient management of records, preservation of records of enduring value, quality access to public information, and data privacy.

#### Scope

HPSD board members and staff.

#### Policy

The HPSD shall retain and dispose of student records in accordance with New Jersey law, and shall comply with active retention schedules for student records per New Jersey's Division of Archive and Record Services.

The HPSD shall expunge student data that is stored upon request of the student if the student is at least 23 years old. The HPSD may expunge medical records and behavioral test assessments. HPSD will not expunge student records of grades, transcripts, a record of the student's enrollment or assessment information. HPSD staff will collaborate with New Jersey State Archives and Records Services in updating data retention schedules.

HPSD maintained student-level discipline data will be expunged after three years.

### **Quality Assurance and Transparency Requirements**

#### Purpose

Data quality is achieved when information is valid for the use to which it is applied, is consistent with other reported data and users of the data have confidence in and rely upon it. Good data quality does not solely exist with the data itself, but is also a function of appropriate data interpretation and use and the perceived quality of the data. Thus, true data quality involves not just those auditing, cleaning and reporting the data, but also data consumers. Data quality is addressed in five areas:

#### Data Governance Structure

The HPSD data governance plan is structured to encourage the effective and appropriate use of educational data. The HPSD data governance structure centers on the idea that data is the responsibility of all HPSD sections and that data driven decision making is the goal of all data collection, storage, reporting and analysis. Data driven decision making guides what data is collected, reported and analyzed.

#### Data Requirements and Definitions

The HPSD members communicate with IT staff regularly, at scheduled Data Governance Team meetings. Where possible, HPSD program specialists are invited to these meetings and the same guidance is given to the appropriate District program directors.

#### Data Collection

Data elements should be collected only once—no duplicate data collections are permitted. Where possible, data is collected at the lowest level available (i.e. at the student/teacher level). Thus, there are no aggregate data collections if the aggregate data can be derived or calculated from the detailed data.

For all new data collections, HPSD provides clear guidelines for data collection and the purpose of the data request. The HPSD also notifies stakeholders as soon as possible about future data collections. Time must be given to the District in order for them to begin gathering the data needed.

### Data Auditing

Data and Statistics Data Analysts perform regular and ad hoc data auditing. They analyze data in the warehouse for anomalies, investigate the source of the anomalies, and work with IT and/or the HPSD in explaining and/or correcting the anomalies. Data Analysts also work with School Finance to address findings from the Auditors.

### Data Transparency

Annually, HPSD will publicly post:

- HPSD data collections

## **Appendix A. HPSD Employee Non-Disclosure Agreement**

**As an employee of the HPSD, I hereby affirm that:** (Initial)

\_\_\_\_\_ I have read the Employee Non-Disclosure Assurances attached to this agreement form and read and reviewed Data Governance Plan HPSD policies. These assurances address general procedures, data use/sharing, and data security.

\_\_\_\_\_ I will abide by the terms of the HPSD's policies and its subordinate process and procedures;

\_\_\_\_\_ I grant permission for the manual and electronic collection and retention of security related information, including but not limited to photographic or videotape images, of your attempts to access the facility and/or workstations.

### **Trainings**

\_\_\_\_\_ I have completed HPSD's Data Security and Privacy Fundamentals Training.

### **Using HPSD Data and Reporting Systems**

\_\_\_\_\_ I will use a password-protected computer when accessing data and reporting systems, viewing child/staff records, and downloading reports.

\_\_\_\_\_ I will not share or exchange individual passwords, for either personal computer(s) or HPSD system user accounts, with HPSD staff or participating program staff.

\_\_\_\_\_ I will log out of and close the browser after each use of HPSD data and reporting systems.

\_\_\_\_\_ I will only access data in which I have received explicit written permissions from the data owner.

\_\_\_\_\_ I will not attempt to identify individuals, except as is required to fulfill job or volunteer duties, or to publicly release confidential data;

### **Handling Sensitive Data**

\_\_\_\_\_ I will keep sensitive data on password-protected state-authorized computers.

\_\_\_\_\_ I will keep any printed files containing personally identifiable information in a locked location while unattended.

\_\_\_\_\_ I will not share child/staff-identifying data during public presentations, webinars, etc. I understand that dummy records should be used for such presentations.

\_\_\_\_\_ I will delete files containing sensitive data after working with them from my desktop, or move them to a secured HPSD server.

## Reporting & Data Sharing

\_\_\_\_\_ I will not re-disclose or share any confidential data analysis except to other authorized personnel without HPSD's expressed written consent.

\_\_\_\_\_ I will not publish any data without the approval of the Superintendent.

\_\_\_\_\_ I will take steps to avoid disclosure of personally identifiable information in state-level reports, such as aggregating, data suppression, rounding, recoding, blurring, perturbation, etc.

\_\_\_\_\_ I will not use email to send screenshots, text, or attachments that contain personally identifiable or other sensitive information. If I receive an email containing such information, I will delete the screenshots/text when forwarding or replying to these messages.

\_\_\_\_\_ I will not transmit child/staff-level data externally unless explicitly authorized in writing.

\_\_\_\_\_ I will immediately report any data breaches, suspected data breaches, or any other suspicious activity related to data access to my supervisor and the HPSD Lead District Technician. Moreover, I acknowledge my role as a public servant and steward of child/staff information, and affirm that I will handle personal information with care to prevent disclosure.

## Consequences for Non-Compliance

\_\_\_\_\_ I understand that access to the HPSD network and systems can be suspended based on any violation of this contract or risk of unauthorized disclosure of confidential information;

\_\_\_\_\_ I understand that failure to report violation of confidentiality by others is just as serious as my own violation and may subject me to personnel action, including termination.

## Termination of Employment

\_\_\_\_\_ I agree that upon the cessation of my employment from HPSD I will not disclose or otherwise disseminate any confidential or personally identifiable information to anyone outside of HPSD without the prior written permission of the Student Data Manager of HPSD.

Print Name: \_\_\_\_\_

Signed: \_\_\_\_\_

Date: \_\_\_\_\_

CERTIFIED RESOLUTION

**9. ACTION - GOVERNANCE AND PERSONNEL**

---

**Subject** 9.30 Approval of HPSD Data Governance Plan

**Meeting** May 14, 2019 - AGENDA

---

**Type** Action (Consent)

**Recommended Action** RESOLVED, that the Board of Education, upon recommendation of the Superintendent, approves the district's Data Governance Plan, as required documentation for the Future Ready Schools certification process and a representation of best-practice.

**Motion & Voting**

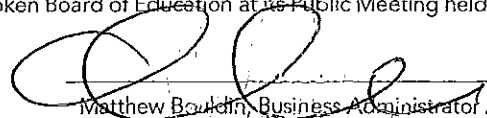
RESOLVED, that the Board of Education approves a Consent Agenda.

Motion by Melanie Tekirian, second by Chetali Khanna.

Final Resolution: Motion Carries

Yes: Malani Cademartori, Sheillah Dallara, Jennifer Evans, Ailene McGuirk, Chetali Khanna, Thomas Kluepfel, Melanie Tekirian, Sharyn Angley

The above is a true copy of a resolution approved by the Hoboken Board of Education at its Public Meeting held on May 14, 2019.

 (Signature)  
Matthew Bouldin, Business Administrator / Board Secretary