HUDSON CITY SCHOOL DISTRICT **POLICY #8635**

(X) Required
(X) Local
(X) Notice

INFORMATION AND DATA PRIVACY, SECURITY, BREACH AND NOTIFICATION

The Board of Education acknowledges the heightened concern regarding the rise in identity theft and the need for secure networks and prompt notification when security breaches occur. The Board adopts the National Institute for Standards and Technology Cybersecurity Framework Version 1.1 (NIST CSF) for data security and protection. The Data Protection Officer is responsible for ensuring the district's systems follow NIST CSF and adopt technologies, safeguards and practices which align with it. This will include an assessment of the district's current cybersecurity state, their target future cybersecurity state, opportunities for improvement, progress toward the target state, and communication about cyber security risk.

The Board will designate a Data Protection Officer to be responsible for the implementation of the policies and procedures required in Education Law §2-d and its accompanying regulations, and to serve as the point of contact for data security and privacy. This appointment will be made at the annual organizational meeting.

The Data Protection Officer shall implement regulations which address:

- the protections of "personally identifiable information," hereinafter referred to as "PPI", of student and teachers/principal under Education Law §2-d and Part 121 of the Commissioner of Education;
- the protections of "private information" under State Technology Law §208 and the NY SHIELD Act; and
- procedures to notify persons affected by breaches or unauthorized access of protected information.

I. Student and Teacher/Principal "Personally Identifiable Information" (PPI) under Education Law §2-d

A. General Provisions

PII as applied to student data is as defined in Family Educational Rights and Privacy Act (Policy 5500, Student Records), which includes certain types of information that could identify a student, and is listed in the accompanying regulation 8635-R. PII as applied to teacher and principal data, means results of Annual Professional Performance Reviews that identify the individual teachers and principals, which are confidential under Education Law §§3012-c and 3012-d, except where required to be disclosed under state law and regulations.

The Data Protection Officer will see that every use and disclosure of personally identifiable information (PII) by the District benefits students and the District (e.g., improve academic achievement, empower parents and students with information, and/or advance efficient and effective school operations). However, PII will not be included in public reports or other documents.

The District will protect the confidentiality of student and teacher/principal PII while stored or transferred using industry standard safeguards and best practices, such as encryption, firewalls, and passwords. The district will monitor its data systems, develop incident response plans, limit access to PII to district employees and third-party contractors who need such access to fulfill their professional responsibilities or contractual obligations, and destroy PII when it is

no longer needed.

Certain federal laws and regulations provide additional rights regarding confidentiality of and access to student records, as well as permitted disclosures without consent, which are addressed in policy and regulation 5500, Student Records.

Under no circumstances will the District sell PII. It will not disclose PII for any marketing or commercial purpose, facilitate its use or disclosure by any other party for any marketing or commercial purpose, or permit another party to do so. Further, the District will take steps to minimize the collection, processing, and transmission of PII.

Except as required by law or in the case of enrollment data, the district will not report the following student data to the State Education Department:

1. juvenile delinquency records;
2. criminal records;
3. medical and health records; and
4. student biometric information.

The district has created and adopted a Parents' Bill of Rights for Data Privacy and Security (see Exhibit 8635-E.1). It has been published on the district's website at hudsoncsd.org and can be requested from the district clerk. The Parents' Bill of Rights will include that:

- Student PII cannot be sold or released for any commercial purposes;
- Parents/guardians have the right to inspect and review the complete contents of their child's education record;
- State and federal laws protect the confidentiality of PII, and that safeguards (such as encryption, firewalls, and passwords) will be in place when data is stored or transferred;
- A complete list of all student data elements collected by the State is available for public viewing, and the web address or mailing address for doing so; and
- Parents/guardians have the right to have complaints about possible breaches of student data addressed, and the contact information to direct those complaints.

For each contract with a third party contractor that receives PII, the Parents' Bill of Rights will include the following supplemental information will include:

- The exclusive purposes for which the PII will be used;
- How the contractor will ensure that subcontractors and/or authorized users will abide by data protection and security requirements;
- The end date of the contract, and what happens to the PII when the contract ends;
- If and how parents/guardians, students, eligible students, teachers or principals may challenge the accuracy of the PII collected;
- Where the PII will be stored (described without compromising data security) and the security measures taken to protect the PII and mitigate security and privacy risks; and
- How the data will be protected using encryption while in motion and at rest.

B. Third-party Contractors

The district will ensure that contracts with third-party contractors that receive protected student and/or teacher or principal data from the District reflect that confidentiality of any student and/or teacher or principal PII be maintained in accordance with federal and state

law and the district's data security and privacy policy.

Each third-party contractor that will receive student data or teacher or principal data must:

1. adopt technologies, safeguards and practices that align with the NIST CSF;
2. comply with the district's data security and privacy policy and applicable laws impacting the district;
3. limit internal access to PII to only those employees or subcontractors that need access to provide the contracted services;
4. not use the PII for any purpose not explicitly authorized in its contract;
5. not disclose any PII to any other party without the prior written consent of the parent or eligible student (i.e., students who are eighteen years old or older):
   a. except for authorized representatives of the third-party contractor to the extent they are carrying out the contract; or
   b. unless required by statute or court order and the third- party contractor provides notice of disclosure to the district, unless expressly prohibited.
6. maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of PII in its custody;
7. use encryption to protect PII in its custody; and
8. not sell, use, or disclose PII for any marketing or commercial purpose, facilitate its use or disclosure by others for marketing or commercial purpose, or permit another party to do so. Third party contractors may release PII to subcontractors engaged to perform the contractor's obligations, but such subcontractors must abide by data protection obligations of state and federal law, and the contract with the district. At least five (5) work days prior to releasing PII to any sub-contractor, the third-party contractor must notify the Data Protection Officer in writing.

Third party contractors may release PII to subcontractors engaged to perform the contractor's obligations, but such subcontractors must abide by data protection obligations of state and federal law, and the contract with the district.

If the third-party contractor has a breach or unauthorized release of PII, it will promptly notify the District in the most expedient way possible without unreasonable delay but no more than seven calendar days after the breach's discovery.

C. Cooperative Educational Services through a BOCES

The District may not be required to enter into a separate contract or data sharing and confidentiality agreement with a third-party contractor that will receive student data or teacher or principal data from the District under all circumstances.

For example, the District may not need its own contract or agreement where:

1. It has entered into a cooperative educational service agreement (CoSer) with a BOCES that includes use of a third-party contractor's product or service; and
2. That BOCES has entered into a contract or data sharing and confidentiality agreement with the third-party contractor, pursuant to Education Law Section 2-d and its implementing regulations, that is applicable to the District's use of the product or service under that CoSer.

To meet its obligations whenever student data or teacher or principal data from the District is received by a third-party contractor pursuant to a CoSer, the District will consult with the BOCES to, among other things:

1. Ensure there is a contract or data sharing and confidentiality agreement pursuant to Education Law Section 2-d and its implementing regulations in place that would specifically govern the District's use of a third-party contractor's product or service under a particular CoSer;
2. Determine procedures for including supplemental information about any applicable contracts or data sharing and confidentiality agreements that a BOCES has entered into with a third-party contractor in its Parents' Bill of Rights for Data Privacy and Security;
3. Ensure appropriate notification is provided to affected parents, eligible students, teachers, and/or principals about any breach or unauthorized release of PII that a third-party contractor has received from the District pursuant to a BOCES contract; and
4. Coordinate reporting to the Chief Privacy Officer to avoid duplication in the event the District receives information directly from a third-party contractor about a breach or unauthorized release of PII that the third-party contractor received from the District pursuant to a BOCES contract.

D. Click-Wrap Agreements

Periodically, District staff may wish to use software, applications, or other technologies in which the user must "click" a button or box to agree to certain online terms of service prior to using the software, application, or other technology. These are known as "click-wrap agreements" and are considered legally binding "contracts or other written agreements" under Education Law Section 2-d and its implementing regulations.

District staff are prohibited from using software, applications, or other technologies pursuant to a click-wrap agreement in which the third-party contractor receives student data or teacher or principal data from the District unless they have received prior approval from the District's Data Protection Officer or designee.

The District will develop and implement procedures requiring prior review and approval for staff use of any software, applications, or other technologies pursuant to click-wrap agreements.

E. Third-Party Contractors' Data Security and Privacy Plan

The district will ensure that contracts with all third-party contractors that receive protected student and/or teacher or principal data from the District include the third-party contractor's data security and privacy plan. This plan must be accepted by the district. At a minimum, each plan will:

1. outline how all state, federal, and local data security and privacy contract requirements over the life of the contract will be met, consistent with this policy;
2. specify the administrative, operation and technical safeguards and practices it has in place to protect PII;
3. demonstrate that it complies with the requirements of 8 N.Y.C.R.R. Section 121.3(c) of the Regulations of the New York Commissioner of Education regarding the supplemental information required to be appended to the Bill of Rights;
4. specify how those who have access to student and/or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;
5. specify if the third-party contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is

protected;

6. specify how the third-party contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the district;
7. describe whether, how and when data will be returned to the district, transitioned to a successor contractor, at the district's option and direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires.

F. Training

The District will provide annual training on data privacy and security awareness to all employees who have access to student and teacher/principal PII.

G. Reporting

Any breach of the District's information storage or computerized data which compromises the security, confidentiality, or integrity of student or teacher/principal PII maintained by the district will be promptly reported to the Data Protection Officer and the Superintendent of Schools. The Superintendent of Schools will promptly notify the Board of Education.

H. Notifications

The Data Protection Officer will report every discovery or report of a breach or unauthorized release of student, teacher or principal PII to the State's Chief Privacy Officer without unreasonable delay, but no more than 10 calendar days after such discovery.

The District will notify affected parents, eligible students, teachers and/or principals in the most expedient way possible and without unreasonable delay, but no more than 60 calendar days after the discovery of a breach or unauthorized release or third-party contractor notification.

However, if notification would interfere with an ongoing law enforcement investigation, or cause further disclosure of PII by disclosing an unfixed security vulnerability, the District will notify parents, eligible students, teachers and/or principals within seven calendar days after the security vulnerability has been remedied, or the risk of interference with the law enforcement investigation ends.

The Board of Education has established regulations which outline procedures to be utilized for the notification of a breach or unauthorized release of student, teacher or principal PII, and has established procedures how to communicate to parents, eligible students, and District staff the process for filing complaints about breaches or unauthorized releases of student and teacher/principal PII. Said procedures are contained in 8635-R, Information and Data Privacy, Breach and Notification Regulations.

II. "Private Information" under State Technology Law §208

"Private information" is defined in State Technology Law §208, and includes certain types of information, outlined in the accompanying regulation, which would put an individual at risk for identity theft or permit access to private accounts. "Private information" does not include information that can lawfully be made available to the general public pursuant to federal or state law or regulation.

Any breach of the District's information storage or computerized data which compromises the security, confidentiality, or integrity of "private information" maintained by the District must be promptly reported to the Data Protection Officer and the Superintendent of Schools. The Superintendent of Schools will promptly notify the Board of Education.

The Board directs the Data Protection Officer, in accordance with appropriate business and technology personnel, to implement regulations which:

- Identify and/or define the types of private information that is to be kept secure;
- Include procedures to identify any breaches of security that result in the release of private information; and
- Include procedures to notify persons affected by the security breach as required by law.

III. Employee "Personal Identifying Information" under Labor Law § 203-d

Pursuant to Labor Law §203-d, the District will not communicate employee "personal identifying information" to the general public. This includes:

1. social security number;
2. home address or telephone number;
3. personal email address;
4. Internet identification name or password;
5. parent's surname prior to marriage; and
6. drivers' license number.

In addition, the District will protect employee social security numbers in that such numbers will not be:

1. publicly posted or displayed;
2. visibly printed on any ID badge, card or time card;
3. placed in files with unrestricted access; or
4. used for occupational licensing purposes.

Employees with access to such information will be notified of these prohibitions and their obligations.

Cross-ref:
1120, District Records
5500, Student Records
8630, Computer Resources and Data Management

Ref:
State Technology Law §§201-208, Labor Law §203-d, Education Law §2-d 8 NYCRR Part 121

Adoption date: January 5, 2021
Review and Re-Adoption date: July 18, 2023
Review & Re-Adoption date: December 16, 2025