Book	Policy Manual
Section	Part VIII - Support Services
Title	Protecting Personal Identifying Information and Notification of Security Breach
Code	8635
Status	Active
Adopted	January 27, 2011
Last Revised	July 9, 2020

8635

INFORMATION AND DATA PRIVACY SECURITY, BREACH AND NOTIFICATION

The Board of Education acknowledges 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 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. 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, the target future cybersecurity state, opportunities for improvement, progress toward the target state, and communication about cyber security risk.

The Superintendent will establish regulations which address:

- the protections of "personally identifiable information" 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 to protected information.

This policy first covers Personally Identifiable Information (PII) for students and teacher/principal under Education Law §2-d and then covers PII for employee under Labor Law §203-d.

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

A. General Provisions

PII, as applied to student data, is defined in Family Educational Rights and Privacy Act (Policy 5500), 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 that the results of Annual Professional Performance Reviews that identify the individual teachers and principals, 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 PII by the District benefits students and the District (e.g., improves academic achievement, empowers parents and students with information, and/or advances 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 in accordance with the records retention Schedule ED-1.

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 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.

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

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

The District has adopted and will update as necessary a Parent’s Bill of Rights for Data Privacy and Security. It will be published on the District’s website and can be requested from the District Clerk.

B. Third-Party Contractors

The District will ensure that contracts with third-party contractors who will receive student and/or teacher or principal data protected by Education Law §2-d will require the 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 receives student, 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 sub-contractors 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.

If the third-party contractor has a breach or unauthorized release of PII, it will immediately notify the District, but no later than seven calendar days after the breach’s discovery.

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

The District will ensure that contracts with all third-party contractors who will receive student and/or teacher or principal data protected by Education Law §2-d include the third-party contractor's data security and privacy plan.

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 safeguards and practices it has in place to protect PII;
3. demonstrate that it complies with the requirements of Section 121.3(c) of the Regulations of the Commissioner of Education;
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 including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the District;
7. describe if, how and when data will be returned to the District, transitioned to a successor contractor, at the District's direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires.

D. 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.

E. 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.

F. Notifications

The Data Protection Officer will immediately report every discovery or report of a breach or unauthorized release of student, teacher or principal PII to the Superintendent and the State's Chief Privacy Officer, but no later 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, but no later 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 Data Protection Officer will establish procedures to provide notification of a breach or unauthorized release of student, teacher or principal PII, and establish and communicate to parents, eligible students, and District staff a process for filing complaints about breaches or unauthorized releases of student and teacher/principal PII.

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 Superintendent who will report it to the Board of Education.

The Superintendent will establish 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.

UNION FREE SCHOOL DISTRICT OF THE TARRYTOWNS

Legal	National Institute for Standards and Technology Cybersecurity Framework Version 1.1 (NIST CSF) 8 NYCRR Part 121 Education Law §2-d State Technology Law §§201-208 Labor Law § 203-d Public Officers Law § 96-a
Cross References	Parents’ Bill of Rights for Student Data, Privacy and Security 5500 - Student Records