INFORMATION AND DATA PRIVACY, SECURITY BREACH AND NOTIFICATION

The Board of Education acknowledges the growing concern regarding the rise in identity theft, the need for secure networks as well as prompt notification when any computer security breach occurs and therefore has adopted the National Institute for Standards and Technology Cybersecurity Framework Version 1.1 (NIST CSF) for data security and protection.

At its annual organizational meeting, the Board will designate a Data Protection Officer (DPO) to be responsible for the implementation of the policies and procedures required in New York State Education Law §2-d and its accompanying regulations, and to serve as the District point of contact for data security and privacy. The DPO is responsible for ensuring the District's systems follow NIST CSF, the policies and procedures required by Education Law §2-d, and for adopting technologies, safeguards and practices that align with it. This will include an assessment of the District's current cybersecurity state, its target future cybersecurity state, opportunities for improvement, progress toward the target state, and communication about cyber security risk.

The Board directs the Superintendent of Schools, in accordance with appropriate business and technology personnel and the DPO, to establish regulations that address:

- the protections of Personally Identifiable Information (PII) of students and teachers/principals under New York State Education Law §2-d and the Part 121 Regulations of the New York State Commissioner of Education;
- the protections of private information under New York State Technology Law §208 and the New York Stop Hacks and Improve Electronic Data Security (SHIELD) Act; and
- procedures to notify persons affected by breaches or unauthorized access of protected information.

I. Student and Teacher/Principal PII under New York State Education Law §2-d

A. General Provisions

PII as applied to student data, defined in the Family Educational Rights and Privacy Act (FERPA) (*Policy 5500 Student Records*), 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 Annual Professional Performance Review (APPR) results that identify the individual teachers and principals which are confidential under New York State Education Law §§3012-c and 3012-d, except where required to be disclosed under New York State law and regulations.

The DPO will ensure that every use and disclosure of PII by the District is legal, appropriate and beneficial to students and the District. PII will not be included in public reports or other documents.

The District will protect the confidentiality of student and teacher/principal PII using industry standard safeguards and best practices. 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 permanently delete 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 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. Additionally, the District will take steps to minimize the collection, processing, and transmission of PII.

Except as required by law, the District will not report the following student data to the New York 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 *Parent's Bill of Rights for Data Privacy and Security (Policy 8635-E)* which is 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 are compliant with Federal and New York State Law, including New York State Education Law §2-d, and this policy regarding confidentiality of any student and/or teacher or principal PII.

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; comply with this policy and applicable laws impacting the District;

2. limit internal access to PII to only those employees or sub-contractors that need access to provide the contracted services;
3. not use the PII for any purpose not explicitly authorized in its contract;
4. not disclose any PII to any other party without the prior written consent of the parent/guardian 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.
5. maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of PII in its custody;
6. use encryption to protect PII in its custody; and
7. not sell, use, or disclose PII for any marketing or commercial purpose, facilitate its use or disclosure by others for any 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 Federal and New York State law, and the contract with the District.

If the third-party contractor or subcontractor has a breach or unauthorized release of PII, it will promptly notify the District no more than 7 calendar days after the breach's discovery, in the most expedient way possible.

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

The District will ensure that contracts with all third-party contractors 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 Federal, New York State, 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 the New York State Commissioner of Education' s Regulations Part 121.3(c);
4. specify how those who have access to student and/or teacher or principal data receive or will receive training on the Federal and New York 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 PII is protected;
6. specify how the third-party contractor will manage data security and privacy incidents that implicate PII 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 and, at the District's direction, permanently deleted by the third-party contractor when the contract is terminated or expires.

D. Training

New York State Education Law §2-d mandates that the District 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 District systems that compromises the security, confidentiality, or integrity of student or teacher/principal PII maintained by the District will be promptly reported to the DPO and the Superintendent of Schools who will then notify the Board of Education.

F. Notifications

The DPO will report every discovery or report of a breach or unauthorized release of student, teacher or principal PII to the New York State Chief Privacy Officer no more than 10 calendar days after such discovery.

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

However, if notification would interfere with an ongoing law enforcement investigation, or cause further disclosure of PII by publicizing a security vulnerability, the District will notify parents/guardians, eligible students, teachers and/or principals within 7 calendar days after the security vulnerability has been remedied, or the risk of interference with the law enforcement investigation ends.

The Superintendent of Schools, in consultation with the DPO, will establish procedures to provide notification of a breach or unauthorized release of student, teacher or principal PII, and establish and communicate to parents/guardians, 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 New York State Technology Law §208

Private information, defined in New York State Technology Law §208, includes certain types of information, outlined in the accompanying regulation (*8635-R*), that 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 New York State law or regulation.

Any breach of District systems that compromise the security, confidentiality, or integrity of private information maintained by the District must be promptly reported to the Superintendent of Schools who will then notify the Board of Education in accordance with the above procedures.

III. Employee Personal Identifying Information under New York State Labor Law §203-d

Pursuant to New York State 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. personal account user names or passwords;
5. parent's/guardian'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 or 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.

Great Neck Public Schools
Adopted: 06/05/06
Amended: 10/17/11; 5/13/20