INFORMATION AND DATA PRIVACY, SECURITY BREACH AND NOTIFICATION

The Board of Education of the Great Neck Public Schools 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.

The District maintains students', teachers' and principals' private information, Personally Identifiable Information (PII), and education records on data management systems and recognizes its responsibility to protect the privacy of student data, including personally identifiable information, and its obligation to notify students and their parents, teachers and principals when a data security breach has/may have resulted in the unauthorized disclosure of, or access to, this information. Therefore, the District has implemented privacy and security measures designed to protect student data stored in its student data management systems (*Policy 8625 Privacy and Security for Student, Teacher and Principal Data*). These measures include reviewing information systems to identify where PII is stored and used, and monitoring data systems to protect against and detect potential breaches. In the event of a breach or suspected breach, the District will promptly take steps to validate the breach, mitigate any loss or damage, and notify law enforcement, if necessary.

Definitions

Private information means personal information (i.e., information such as name, number, symbol, mark or other identifier which can be used to identify a person) in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:

- Social security number;
- Driver's license number or non-driver identification card number; or
- Account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account; or
- Biometric information (data generated by electronic measurements of a person's physical characteristics, such as finger print, voice print, retina image or iris image) used to authenticate or ascertain a person's identity.

Private information does not include publicly available information that is lawfully made available to the general public pursuant to New York State or Federal law or regulation.

The Board 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 will

- Identify and/or define the types of private information that is to be kept secure. For purposes of this policy, "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;
- Address 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
- Include procedures to identify any breaches of security that result in the release of private information; and
- Include procedures to notify persons affected by breaches or unauthorized access of protected information as required by law.

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 electronic email address;
4. Internet identification names or passwords;
5. parent's/guardian's surname prior to marriage;
6. or 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 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.

If the District determines that a security breach has occurred, affected individuals will be provided notice without unreasonable delay. The notification method may vary depending on the type of data breached and the number of individuals affected and the Superintendent of Schools will be responsible for implementing an appropriate response.

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.

Breach of the security of the system means unauthorized acquisition or acquisition without valid authorization of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the District. Good faith acquisition of personal information by an officer or employee or agent of the District for the purposes of the District is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.

To successfully implement this policy, the District will inventory its computer programs and electronic files to determine the types of personal, private information that is maintained or used by the District, and review the safeguards in effect to secure and protect that information.

Procedure for Identifying Security Breaches

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, the District may consider the following factors, among others:

1. indications that an unauthorized person is in physical possession or control of the information, such as a lost or stolen computer, or other device containing information;
2. indications that an unauthorized person downloaded or copied the information;
3. indications that an unauthorized person used the information , such as fraudulent accounts opened or instances of identity theft reported; and/or
4. any other factors that the District deems appropriate and relevant to such determination.

Security Breaches – Procedures and Methods for Notification

Once it has been determined that a security breach has occurred, the following steps will be taken:

1. If the breach involved computerized data *owned or licensed* by the District, the District will notify those New York State residents whose private information was, or is reasonably believed to have been acquired by a person without valid authorization. The disclosure to affected individuals will be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system. The

District will consult with the New York State Office of Information Technology Services to determine the scope of the breach and restoration measures. In addition, the District will consult with the New York State Office of Cyber Security and Critical Infrastructure Coordination (CSCIC) to determine the scope of the breach and restoration measures.

2. If the breach involved computer data maintained by the District, the District will notify the owner or licensee of the information of the breach immediately following discovery, if the private information was or is reasonably believed to have been acquired by a person without valid authorization.
3. In the event a third party doing business with the District experiences a breach of its data security and/or privacy of students, teachers or principals and/or unauthorized release of student data, the third party will immediately notify the District and advise it as to the nature of the breach and the steps it has taken to minimize said breach. Said notification must be made within seven (7) days of the breach. In the case of required notification by the District to a parent, student, teacher or principal, the third party will promptly reimburse the District for the full cost of such notification.
4. In the event that the third party fails to notify the District of a breach, said failure will be punishable by a civil penalty of the greater of $5,000 or up to $20 per student, teacher and principal whose data was released, provided that the maximum penalty imposed will not exceed the maximum penalty imposed under New York State General Business Law, section 899-aa(6)(a).
5. In the event the third party violates New York State Education Law 2-d, said violation will be punishable by a civil penalty of up to $1,000. A second violation involving the same data will be punishable by a civil penalty of up to $5,000. Any subsequent violation involving the same data will be punishable by a civil penalty of up to $10,000. Each violation will be considered a separate violation for purposes of civil penalties and the total penalty cannot exceed the maximum penalty imposed under New York State General Business Law section 899-aa(6)(a).

The notification requirement may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The required notification will be made after the law enforcement agency determines that such notification does not compromise the investigation.

Notifications will be clear, concise, use language that is plain and easy to understand, and to the extent available, include:

a. A brief description of the breach or unauthorized release, the dates of the incident and the date of discovery, if known;
b. A description of the types of PII affected;
c. An estimate of the number of records affected;
d. A brief description of the District's investigation or plan to investigate;
e. Contact information for representatives who can assist parents or eligible students, teachers or principals that have additional questions; and

f. The telephone number and website of relevant New York State and Federal agencies that provide information on security breach response and identity theft protection and prevention.

This notice will be directly provided to the affected individuals by either:

1. Written notice;
2. Electronic notice, provided that:
   a) the person to whom notice is required has expressly consented to receiving the notice in electronic form;
   b) the District keeps a log of each such electronic notification. In no case, however, will the District require a person to consent to accepting such notice in electronic form as a condition of establishing a business relationship or engaging in any transaction; or
3. Telephone notice, provided that the District keeps a log of each such telephone notice.

However, if the District can demonstrate to the New York State Attorney General that (a) the cost of providing notice would exceed $250,000; or (b) that the number of persons to be notified exceeds 500,000; or (c) that the District does not have sufficient contact information, substitute notice may be provided. Substitute notice would consist of all of the following steps:

1. E-mail notice when the District has such an address for the affected individual;
2. Conspicuous posting on the District's website, if one is maintained; and
3. Notification to major media.

If the District has already notified affected persons under any other Federal or New York State laws or regulations regarding data breaches, including the Federal Health Insurance Portability and Accountability Act (HIPAA), the Federal Health Information Technology for Economic and Clinical Health (HI TECH) Act, or New York State Education Law §2-d, it is not required to notify them again. Notification to New York State and other agencies is still required.

Notification of State and Other Agencies

Once notice has been made to affected New York State residents, the District will notify the New York State Attorney General, the New York State Consumer Protection Board, the New York State Office of Information Technology Services and the New York State Office of Cyber Security and Critical Infrastructure Coordination as to the timing, content, and distribution of the notices and approximate number of affected persons.

If more than 5,000 New York State residents are to be notified at one time, the District will also notify consumer reporting agencies as to the timing, content and distribution of the notices and the approximate number of affected individuals. A list of consumer reporting agencies will be furnished, upon request, by the Office of the New York State Attorney General.

If the District is required to notify the U.S. Secretary of Health and Human Services of a breach of unsecured protected health information under the Federal Health Insurance Portability and Accountability Act (HIPAA) or the Federal Health Information Technology for Economic and Clinical Health (HI TECH) Act, it will also notify the New York State Attorney General within five (5) business days of notifying the U. S. Secretary.

In addition, the District will report every discovery or report of a breach or unauthorized release of student data or teacher or principal (PII) maintained by the District to the New York State Chief Privacy Officer without unreasonable delay, but no more than ten (10) calendar days after such discovery.

Each third-party contractor that receives student data or teacher or principal data pursuant to a contract or other written agreement entered into with the District will be required to promptly notify the District of any breach of security resulting in an unauthorized release of the data by the third-party contractor or its assignees in violation of applicable laws and regulations, the Parents' Bill of Rights for Student Data Privacy and Security, District policy, and/or binding contractual obligations relating to data privacy and security, in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after the discovery of the breach.

In the event of notification from a third-party contractor, the District will in turn notify the New York State Chief Privacy Officer of the breach or unauthorized release of student data or teacher or principal data no more than ten calendar days after it receives the third-party contractor's notification using a form or format prescribed by the New York State Education Department.

Annual Data Privacy and Security Training

New York State Education Law §2-d mandates that the District provide annual training on data privacy and security awareness to its officers and staff who have access to student and teacher/principal PII. This training will include, but not be limited to, training on the applicable laws and regulations that protect PII and how staff can comply with these laws and regulations. The District may deliver this training using online training tools. Additionally, this training may be included as part of the training that the District already offers to its workforce.

Great Neck Public Schools
Adopted: 06/05/06
Amended: 10/17/11; 5/13/20, 3/9/22