NORTH MERRICK UNION FREE SCHOOL DISTRICT

INFORMATION SECURITY BREACH AND NOTIFICATION

Policy 2635

The School District maintains students', teachers' and principals' private information, personally identifiable information, 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 School District has implemented privacy and security measures designed to protect student data stored in its student data management systems. These measures include reviewing information systems to identify where personally identifiable information 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 School District will promptly take steps to validatethe breach, mitigate any loss or damage, and notify law enforcement, if necessary.

To this end, the Superintendent of Schools or his/her designee, in accordance with appropriate business and technology personnel, 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 state law or regulation;
- 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;

Additionally, pursuant to Labor Law §203-d, the School District will not communicate employee and student "personally identifying information" to the general public. This includes social security number, home address or telephone number, personal electronic email address, Internet identification name or password, parent's surname prior to marriage, or driver's license number. In addition, the School District will protect employee social security numbers in that such numbers shall not: be publicly posted or displayed, be printed on any ID badge, card or time card, be placed in files with unrestricted access, or be used for occupational licensing purposes. Employees with access to such information shall be notified of these prohibitions and their obligations.

If the School 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 will be responsible for implementing an appropriate response. To this end, the Superintendent of Schools or his/her designee, in accordance with appropriate business and technology personnel, 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 state law or regulation;

- 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;

Any breach of the School District's computerized data which compromises the security, confidentiality, or integrity of personal information maintained by the School District shall be promptly reported to the Superintendent of Schools and the Board of Education.

Definitions

"Private information" shall mean 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.

Note: "Private information" does not include publicly available information that is lawfully made available to the general public pursuant to state or federal law or regulation.

"Breach of the security of the system" shall mean unauthorized acquisition or acquisition without valid authorization of computerized data which compromises the security, confidentiality, or integrity of personal information maintained by the School District. Good faith acquisition of personal information by an officer or employee or agent of the School District for the purposes of the School 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 School District shall inventory its computer programs and electronic files to determine the types of personal, private information that is maintained or used by the School 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 School 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 which the School District shall deem 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 shall be taken:

1. If the breach involved computerized data *owned or licensed* by the School District, the School District shall 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 shall 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 School 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 School District shall 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 School District, the School District shall 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 School 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 shall immediately notify the School 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 School District to a parent, student, teacher or principal, the third party shall promptly reimburse the School District for the full cost of such notification.

Third-party contractors must cooperate with educational agencies and law enforcement to protect the integrity of investigations into the breach or unauthorized release of personally identifiable information.

4. In the event that the third party fails to notify the School District of a breach, said failure shall be punishable by a civil penalty of the greater of $5,000 or up to $10 per student, teacher and principal whose data was released, provided that the maximum penalty imposed shall not exceed the maximum penalty imposed under General Business Law, section 899-aa(6)(a).

5. In the event the third party violates Education Law 2-d, said violation shall be punishable by a civil penalty of up to $1,000. A second violation involving the same data shall be punishable by a civil penalty of up to $5,000. Any subsequent violation involving the same data shall be punishable by a civil penalty of up to $10,000. Each violation shall be considered a separate violation for purposes of civil penalties and the total penalty shall not exceed the maximum penalty imposed under General Business Law section 899-aa(6)(a).
6. The Chief Privacy Officer shall investigate reports of breaches or unauthorized releases of student data or teacher or principal data by third-party contractors. As part of an investigation, the Chief Privacy Officer may require that the parties submit documentation, provide testimony, and may involve visit to, or examination and inspection of the third-party contractor's facilities and records by the Chief Privacy Officer.
7. Upon conclusion of an investigation, if the Chief Privacy Officer determines that a third-party contractor has through its actions or omissions caused student data or teacher or principal data to be breached or released to any person or entity not authorized by law to receive such data in violation of applicable state or federal law, the data and security policies of the educational agency, and/or any binding contractual obligations, the Chief Privacy Officer shall notify the third-party contractor of such finding and give the third-party contractor no more than 30 days to submit a written response.
8. State Chief Privacy Officer Roles and Responsibilities:
   a) order the third-party contractor be precluded from accessing personally identifiable information from the affected educational agency for a fixed period of up to five years; and/or
   b) order that a third-party contractor or assignee who knowingly or recklessly allowed for the breach or unauthorized release of student data or teacher or principal data be precluded from accessing student data or teacher or principal data from any educational agency in the state for a fixed period of up to five years; and/or
   c) order that a third party contractor who knowingly or recklessly allowed for the breach or unauthorized release of student data or teacher or principal data shall not be deemed a responsible bidder or offeror on any contract with an educational agency that involves the sharing of student data or teacher or principal data, as applicable for purposes of the provisions of General Municipal Law §103 or State

Finance Law §163(10)(c), as applicable, for a fixed period of up to five years;

d) require the third-party contractor to provide additional training governing confidentiality of student data and/or teacher or principal data to all its officers and employees with reasonable access to such data and certify that it has been performed, at the contractor's expense. Such additional training must be performed immediately and include a review of federal and state laws, rules, regulations, including Education Law §2-d and this Part.

Note: The notification requirement may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The required notification shall 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 School 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 state and federal agencies that provide information on security breach response and identity theft protection and prevention.

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

1. Written notice;

2. Electronic notice, provided that the person to whom notice is required has expressly consented to receiving the notice in electronic form; and that the School District keeps a log of each such electronic notification. In no case, however, shall the School 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 notification, provided that the School District keeps a log of each such telephone notification.

However, if the School District can demonstrate to the 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 School 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 School District has such address for the affected individual;
2. Conspicuous posting on the School District's website, if they maintain one; and
3. Notification to major media.

If the School District has already notified affected persons under any other federal or state laws or regulations regarding data breaches, including the federal Health Insurance Portability and Accountability Act, 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 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 School District shall notify the State Attorney General, the Consumer Protection Board, the State Office of Information Technology Services and the 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 School District shall 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 State Attorney General.

If the School 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 State Attorney General within five (5) business days of notifying the Secretary.

In addition, the School District will report every discovery or report of a breach or unauthorized release of student data or teacher or principal data within the School District to the Chief Privacy Officer without unreasonable delay, but no more than ten calendar days after the 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 School District will be required to promptly notify the School 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, School 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 calendar days after the discovery of the breach.

In the event of notification from a third-party contractor, the School District will in turn notify the 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

The School District will annually provide data privacy and security awareness training to its officers and staff with access to 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 School District may deliver this training using online training tools. Additionally, this training may be included as part of the training that the School District already offers to its workforce.

Notification of Policy

The School District will publish this policy on its website and provide notice of the policy to all its officers and staff.

Cross-Ref: Policy 2625 Privacy and Security for Student, Teacher and Principal Data

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

Adoption date: January 12, 2021
Revised/adopted: July 11, 2023