INFORMATION SECURITY BREACH AND NOTIFICATION

The Board of Education acknowledges the heightened concern regarding the rise in identity theft and the theft of private information and the need for secure networks and prompt notification when security breaches occur. To this end, the Board directs the Superintendent of Schools, in accordance with appropriate business and technology personnel, to establish regulations which:

- 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.
- Include procedures to notify persons affected by the security breach as required by law.

Additionally, pursuant to Labor Law §203-d, the District will not communicate employee "personal identifying information" to the general public. This includes social security number, home address or telephone number, personal health information, personal electronic email address, internet identification name, parent's surname prior to marriage, or driver's license number. The 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.

"Breach of the security of the system" shall mean unauthorized acquisition or acquisition without valid authorization of physical or computerized data which 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

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

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

Reference: State Technology Law §§ 201-208
Labor Law § 203-d
HIPAA 45 CFR §§ 164.400-414

Adopted: October 23, 2018

INFORMATION SECURITY BREACH AND NOTIFICATION REGULATION

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.
- 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.

To successfully implement this policy, the District shall inventory its hard copy, 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 shall consider:

1. indications that the information is in the physical possession and control of an unauthorized person, such as removal of hard copies, lost or stolen computer, or other device containing information

2. indications that the information has been downloaded, removed or copied

3. indications that the information was used by an unauthorized person, such as fraudulent accounts, opened or instances of identity theft reported

4. any other factors which the District shall deem appropriate and relevant to such determination

Security Breaches – Procedures and Methods for Notification

Investigation of Breaches

Breach investigations will be conducted by the Assistant Superintendent of Human Resources, Safe Schools & IT, Supervisor of Instructional Technology, or a designee of the Superintendent. If necessary, law enforcement should be contacted when a breach is detected. Steps to be taken in a breach investigation may include:

1. Determine exactly what information was compromised (i.e., names, addresses, contact information, social security numbers, student or employee ID numbers, credit/debit card numbers, grades, birth dates, passwords).

2. Take immediate steps to retrieve data and prevent any further unauthorized disclosures.

3. Identify all affected records and students and/or employees.

4. Determine how the incident occurred, including which school officials had control of and responsibility for the information that was compromised.

5. Determine whether institutional policies and procedures were breached, including organizational requirements governing access (user names, passwords, PINs, etc.), storage, encryption, transmission, and destruction of information from education records.

6. Determine whether the incident occurred because of a lack of monitoring and oversight.

7. Conduct a risk assessment and identify appropriate physical, technological, and administrative measures to prevent similar incidents in the future.

8. Determine when the breach occurred.

9. Determine which devices or networks were involved.

10. Determine if a data encryption key was compromised.

11. Clarify the scope of the breach and the individuals involved (i.e., did it affect a specific, identifiable group of individuals on the District's network or was it random?).

12. Determine if the breach also involved additional cyber incidents such as denial of service, scans or malicious code.

The District should utilize a back-up system to ensure continuity of operations as deemed appropriate.

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

1. If the breach involved hard copy or computerized data <u>owned or licensed</u> by the District, the 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 District shall consult with the New York State Office of Cyber Security and Critical Infrastructure Coordination (CSCIC) (https://its.ny.gov/eiso) to determine the scope of the breach and restoration measures.

2. If the breach involved hard copy or computer data maintained by the District, the 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.

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.

The required notice shall include:

(a) District contact information
(b) a description of the categories information that were or are reasonably believed to have been acquired without authorization
(c) which specific elements of personal or private information were or are reasonably believed to have been acquired
(d) a description of what the District is doing about it

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 District keeps a log of each such electronic notification. In no case, however, shall 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.

3. Telephone notification, provided that the District keeps a log of each such telephone notification.

However, if the 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 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 address for the affected individual
2. conspicuous posting on the District's website
3. notification to major media

Notification of State and Other Agencies

The District shall provide awareness training to employees in regard to the process for reporting a breach or a suspected breach.

Once notice has been made to affected New York State residents, the District shall notify the State Attorney General, the Department of State Division of Consumer Protection, and the State Office of Information Technology Services 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 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.

Issued: October 23, 2018

NEW YORK STATE SECURITY BREACH REPORTING FORM
Pursuant to the Information Security Breach and Notification Act
(General Business Law §899-aa)

Name and address of Entity that owns or licenses the computerized data that was subject to the breach:
_____
Street Address: _____
City: _____ State: _____ Zip Code: _____

Submitted by: _____ Title: _____ Dated: _____
Firm Name (if other than entity): _____
Telephone: _____ Email: _____
Relationship to Entity whose information was compromised: _____

Type of Organization (please select one):
[ ] Governmental Entity in New York State; [ ] Other Governmental Entity; [ ] Educational; [ ] Health Care;
[ ] Financial Services; [ ] Other Commercial; [ ] Not-for-profit

Number of Persons Affected:
Total (Including NYS residents): _____ NYS Residents: _____
If the number of NYS residents exceeds 5,000, have the consumer reporting agencies been notified? [ ] Yes; [ ] No.

Dates: Breach Occurred: _____ Breach Discovered: _____ Consumer Notification: _____

Description of Breach (please select all that apply):
[ ] Loss or theft of device or media (e.g., computer, laptop, external hard drive, thumb drive, CD, tape);
[ ] Internal system breach; [ ] Insider wrongdoing; [ ] External system breach (e.g., hacking);
[ ] Inadvertent disclosure; [ ] Other
(specify):_____

Information Acquired: Name or other personal identifier in combination with (please select all that apply):
[ ] Social Security Number
[ ] Driver's license number or non-driver identification card number
[ ] Financial account number or credit or debit card number, in combination with the security code, access code, password, or PIN for the account

Manner of Notification to Affected Persons - ATTACH A COPY OF THE TEMPLATE OF THE NOTICE TO AFFECTED NYS RESIDENTS:
[ ] Written; [ ] Electronic; [ ] Telephone; [ ] Substitute notice.
List dates of any previous (within 12 months) breach notifications: _____

Identify Theft Protection Service Offered: [ ] Yes; [ ] No.
Duration: _____ Provider: _____
Brief Description of Service: _____

NEW YORK STATE SECURITY BREACH REPORTING FORM
Pursuant to the Information Security Breach and Notification Act
(General Business Law §899-aa)

Please complete and submit this form to each of the three state agencies listed below:

Fax or Email this form to:

New York State Attorney General's Office
SECURITY BREACH NOTIFICATION
Consumer Frauds & Protection Bureau
120 Broadway – 3rd Floor
New York, NY 10271
Fax: 212-416-6003
Email: breach.security@ag.ny.gov

New York State Division of State Police
SECURITY BREACH NOTIFICATION
New York State Intelligence Center
31 Tech Valley Drive, Second Floor
East Greenbush, NY 12061
Fax: 518-786-9398
Email: risk@nysic.ny.gov

New York State Department of State Division of Consumer Protection
Attention: Director of the Division of Consumer Protection
SECURITY BREACH NOTIFICATION
99 Washington Avenue, Suite 650
Albany, New York *12231*
Fax: (518) 473-9055
Email: security_breach_notification@dos.ny.gov

To access the most recent online version of the NYS Security Breach Reporting Form:
https://its.ny.gov/breach-notification

NYS Security Breach Reporting Form used with permission from the New York State Office of Cyber Security.