

Book	Policy Manual
Section	8000 - Support Services
Title	Information Security Breach and Notification
Code	8635
Status	Active
Legal	Reviewed by Counsel December 4, 2014
Adopted	January 11, 2018
Last Revised	December 13, 2017
Last Reviewed	December 13, 2017

The Board of Education acknowledges the State’s concern regarding the rise in identity theft and the need for prompt notification when security breaches occur.

The School District maintains students' private information, personally identifiable information, and education records on its student 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 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. 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 validate the breach, mitigate any loss or damage, and notify law enforcement, if necessary.

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 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.

Additionally, pursuant to Labor Law §203-d, the School District will not communicate employee “personal 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.

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.

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 shall consider:

1. indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer, or other device containing information;
2. indications that the information has been downloaded or copied;
3. indications that the information was used by an unauthorized person, 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.
2. 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.
3. 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.

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.

The required notice shall include (a) School District contact information, (b) a description of the categories information that were or are reasonably believed to have been acquired without authorization and (c) which specific elements of personal or private information were or are reasonably believed to have been acquired. 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.
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.

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, 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.

Cross-ref:

5500 Student Records
5550 Student Privacy
9160 Personnel Records

Ref:

State Technology Law §§201-208
Labor Law §203-d