INFORMATION SECURITY BREACH AND NOTIFICATION

The Board of Education acknowledges the heightened concern regarding the rise in identity theft 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, which will include all "personally identifiable information" of students, and District employees under Education Law §2-d and Part 121 of the regulations of the Commissioner of Education. 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 ofprivate information; and
- 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 but is not limited to social security number, home address or telephone number, personal email address, Internet identification name or password, parent's surname prior to marriage, or driver's license number. In addition, 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.

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 Data Protection Officer, the Superintendent and the Board of Education.

Cross-ref: 1111, Public Access to School District Records
1310, Release of Information about Staff Members, School Volunteers and Students
3802, Technology Security for Personal, Private and Sensitive Information
4410, Technology Acceptable Use Policy
4411, Remote Access to Computer Network
4420, Computer Controls Policy for Financial Software
5125, Availability of Student Records in Accordance with the Family Educational Rights and Privacy Act of 1974
6147, Technology Acceptable Use Policy (Students)

Information Security Breach and Notification (Continued)

Ref: State Technology Law §§201-208
Labor Law §203-d
Education Law 2-d

Adoption date:
August 21, 2014
Reviewed:
October 24, 2016
Reviewed:
August 28, 2017
Reviewed:
August 27, 2018
Revised:
June 29, 2020
Reviewed:
October 24, 2022
Revised:
August 21, 2023
Revised:
September 16, 2024

INFORMATION SECURITY BREACH AND NOTIFICATION REGULATION

Definitions

"Private information" shall mean all "Personally Identifiable Information" for students, teachers, principals, and District employees as defined under Education Law §2-d and Part 121 of the Regulations of the Commissioner of Education.

"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.

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

1. 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: 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; and/or
4. any other factors which the 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 hard copy or computerized data *owned or licensed* 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.

Information Security Breach and Notification – Regulation (Continued)

The 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 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.
3. The District must report any breach or unauthorized release of personally identifiable information to the Commissioner of Education's Chief Privacy Officer within 10 calendar days of any discovery or any notification by a third-party.
4. The District must also notify by first-class mail, by email, or by telephone the affected parents, eligible students, teachers, and principals in the most expedient way, but no more than 60 days after the discovery of the breach.

The required notice must be clear, concise, use language that is plain and easy to understand and shall include a brief description of the breach or unauthorized release, the dates of the incident and the date of discovery, if known; a description of the types of personally identifiable information affected; an estimate of the number of records affected; a brief description of the educational agency's investigation or plan to investigate; and contact information for representatives who can assist parents or eligible students that have additional questions. 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 individuals;
2. Conspicuous posting on the district's website; and
3. Notification to major media.

Information Security Breach and Notification – Regulation (Continued)

Security Breaches – Complaint Procedure

The following complaint procedure is established pursuant to Education Law §2-d and Part 121.4 of the Regulations of the Commissioner of Education. All parents, eligible students, teachers, principals, and District employees of an educational agency may submit in writing a complaint alleging breaches or unauthorized releases of student data. The complaints may be submitted to the Data Protection Officer or any District employee, who then must notify the Data Protection officer. The District must promptly acknowledge receipt of complaints, commence an investigation, and take the necessary precautions to protect personally identifiable information. Following the investigation, the District will provide the complainant with its findings within 60 calendar days from the receipt of the complaint. Where additional time is necessary or the response may compromise security or impede a law enforcement investigation the District shall provide a written explanation that includes the approximate date when the educational agency anticipates that it will respond. The District must maintain a record of all complaints filed and their disposition.

Notification of State and Other Agencies

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.

Adoption date:
August 21, 2014
Reviewed:
October 24, 2016
Reviewed:
August 28, 2017
Reviewed:
August 27, 2018
Revised:
June 29, 2020
Reviewed:
October 24, 2022
Reviewed:
August 21, 2023
Reviewed:
September 16, 2024