5672 - Information Security Breach and Notification

2011 5672

Non-Instructional/Business Operations

SUBJECT: INFORMATION SECURITY BREACH AND NOTIFICATION

The School District values the protection of private information of individuals in accordance with applicable law and regulations. Further, the District is required to notify affected individuals when there has been or is reasonably believed to have been a compromise of the individual's private information in compliance with the Information Security Breach and Notification Act and Board policy.

a) "*Private information*" shall mean ***personal information* in combination with any one (1) 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:

1. Social security number;

2. Driver's license number or non-driver identification card number; or

3. 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.

"*Private information*" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.

**"*Personal information*" shall mean any information concerning a person which, because of name, number, symbol, mark or other identifier, can be used to identify that person.

b) "*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 District. Good faith acquisition of personal information by an employee or agent of the District for the purposes of the District is not a breach of the security of the system, provided that private information is not used or subject to unauthorized disclosure.

Examples of Determining Factors

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

factors, among others:

a) 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; or

b) Indications that the information has been downloaded or copied; or

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

Notification Requirements

a) For any computerized data owned or licensed by the School District that includes private information, the District shall disclose any breach of the security of the system following discovery or notification of the breach to any New York State resident 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 restore the reasonable integrity of the data system. The District shall consult with the State Office of Information Technology Services to determine the scope of the breach and restoration measures.

b) For any computerized data maintained by the District that includes private information which the District does not own, the District shall notify the owner or licensee of the information of any breach of the security of the system 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.

Methods of Notification

The required notice shall be directly provided to the affected persons by one (1) of the following methods:

a) Written notice;

b) Electronic notice, provided that the person to whom notice is required has expressly consented to receiving the notice in electronic form; and a log of each such notification is kept by the District when notifying affected persons in electronic form. However, in no case shall the District require a person to consent to accepting such notice in electronic form as a condition of establishing any business relationship or engaging in any transaction;

c) Telephone notification, provided that a log of each such notification is kept by the District when notifying affected persons by phone; or

d) Substitute notice, if the District demonstrates to the State Attorney General that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or that the District does not have sufficient contact information. Substitute notice shall consist of **all** of the following:

1. E-mail notice when the District has an e-mail address for the subject persons;

2. Conspicuous posting of the notice on the District's website page, if the District maintains one; and

3. Notification to major statewide media.

Regardless of the method by which notice is provided, the notice shall include contact information for the notifying District and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired.

In the event that any New York State residents are to be notified, the District shall notify the State Attorney General, the New York State Department of State, and the State Office of Information Technology as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York State residents.

In the event that more than five thousand (5,000) New York State residents are to be notified at one time, the District shall also notify consumer reporting agencies, as defined pursuant to State Technology Law Section 208, as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York State residents. A list of consumer reporting agencies shall be compiled by the State Attorney General and furnished upon request to school districts required to make a notification in accordance with State Technology Law Section 208(2), regarding notification of breach of security of the system for any computerized data owned or licensed by the District that includes private information.

State Technology Law Sections 202 and 208

Adopted: 4/11/11