SUPPORT OPERATIONS 5304

INFORMATION SECURITY BREACH POLICY

I. Statement of Policy

The District takes reasonable administrative, technical, and physical measures to protect the security of private information, as defined in State Technology Law Section 208, held in the District's digitally-stored records. If the District learns of a breach of the security of its digitally-stored records, the District notifies affected data subjects as set forth in this Policy, and also notifies the appropriate State agencies. This Policy applies to information stored by the District or stored by a third party on behalf of the District.

II. Scope of Information Protected

A. Information that is Protected

1. In connection with any software platform or application that requires the creation of a user account with a password, disclosure of the user name or email address in combination with a password or security question and answer that would permit access to an online account is considered disclosure of private information.

2. Private information also is deemed to have been disclosed if the following conditions are met:

   a. one of the following data elements related to the data subject has been disclosed:

      i. social security number, or

      ii. driver's license number or non-driver identification card number, or

      iii. account number, credit or debit card number, in combination with any required security code, access code, password, or other information which would permit access to an individual's financial account, or

      iv. account number, or credit or debit card number, if circumstances exist where such number could be used to access an individual's financial account without additional identifying information, security code, access code, or password, or

      v. biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as fingerprint, voice print, or retina or iris image, or other unique physical representation or digital representation which are used to authenticate or ascertain the individual's identity; and

b. any other information about the data subject has been disclosed, and

c. either the data element or the combination of personal information plus the data element is not encrypted or is encrypted with an encryption key that has also been accessed or acquired.

B. Information Not Covered by This Policy

1. Publicly available information that is lawfully made available to the general public from Federal, State, or local governmental records is not private information within the meaning of this Policy.

2. Personally identifiable information of students, eligible students, and teachers or principals governed by Education Law Section 2-d is managed by the District, and data breach notifications are provided, in accordance with Policy 5306 and is not private information within the meaning of this Policy.

III. When Notification is Required

A. General Rule

The District shall provide notification of any breach of its system for storing private information following discovery or notification of the breach of the security of the system to any resident of New York State whose private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization.

B. Determining Whether a Breach of Security Occurred

1. "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 private information maintained by the District.

2. 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 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.

C. Inadvertent Disclosure by Authorized Persons

Notice to affected persons under this Policy is not required if the exposure of private information was an inadvertent disclosure by persons authorized to access private information, and the District reasonably determines such exposure will not likely result in misuse of such information, or financial or emotional harm to the affected persons. Such a determination shall be documented in writing and maintained for at least five years. If the incident affected over five hundred residents of New York, the District/BOCES shall provide the written determination to the state attorney general within ten days after the determination.

IV. Notification Procedures

A. Notification Methods

The District will notify the affected data subject(s) by one of the following methods:

1. written notice;

2. electronic notice, provided that the person to whom the notice is required has expressly consented to receiving said notice in electronic form; a log of each such notification shall be kept by the District;

3. telephone notification; a log of each such notification shall be kept by the District;

4. substitute notice, if the cost of providing notice would exceed two hundred fifty thousand dollars, or the affected class of persons to be notified exceeds five hundred thousand, or the District does not have sufficient contact information. Substitute notice shall consist of all of the following:

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

b. conspicuous posting of the notice on the District's web site page, if the District maintains one; and

c. notification to major District-wide media.

B. Notification Content

The notice must include the District's contact information, and a description of the categories of information that were, or are reasonably believed to have been, accessed or acquired by a person without valid authorization, including specification of which elements of private information were, or are reasonably believed to have been, accessed or acquired. The notice shall also include the telephone numbers and website addresses of state and federal agencies that provide information regarding security breach response and identity theft prevention and protection information.

C. Notification Timing

Disclosure of the unauthorized access to or acquisition of private information shall be made in the most expedient time possible and without unreasonable delay, consistent with the needs of law enforcement and the measures necessary to first determine the scope of the breach and restore the integrity of the information storage system.

D. Coordination with Law Enforcement

Notification may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The notification required shall be made after such law enforcement agency determines that such notification does not comprise such investigation.

V. Other Notifications

When notification of individual data subjects is necessary, the District shall also notify the New York State Attorney General, the New York Department of State, and the New York State Office of Information Technology Services, providing them with information about the timing, content, and distribution of the notices and approximate number of affected persons. If more than 5,000 New York State residents are required to be notified of a particular incident, the District will also notify consumer reporting agencies with the same information and without waiting to complete notifications to the individual affected data subjects.

Bainbridge-Guilford Central School District
Legal Ref: NYS State Technology Law §208,
Adopted: 05/02/13
Revised: 01/11/18, 06/04/20