

INFORMATION SECURITY BREACH AND NOTIFICATION

The Board of Education of the Valley Stream Union Free School District Twenty-Four acknowledges the rise in identity theft and the need for 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; and
- Include procedures to notify persons affected by the security breach as required by law.

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

First Reading: June 14, 2007

Adoption date: July 9, 2007

INFORMATION SECURITY BREACH AND NOTIFICATION REGULATION

Definitions

“Private information” means personal information (e.g., 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” means 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 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.

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 will 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 District deems appropriate and relevant to its 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 District, the District will 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 will 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 computer data *maintained* by the District, the District will 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 the notification impedes a criminal investigation. The required notification will be made after the law enforcement agency determines that this notification will not compromise the investigation.

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

If, however, 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 this address for the affected individual;
2. Conspicuous posting on the District's website, if the District maintains 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 District will 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 District will 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.

First Reading: June 14, 2007

Adoption date: July 9, 2007