INFORMATION SECURITY BREACH AND NOTIFICATION REGULATION

The Board of Education (the Board) of the Bethlehem Central School District (the District) acknowledges the state's concern regarding the rise in identity theft and the need for prompt notification when security breaches occur. To this end, the Board directs the superintendent, in accordance with appropriate business and technology personnel, to establish regulations that:

Definitions

“Private information” shall mean personal information (i.e., information such as name, number, symbol, mark, or other identifiers that 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:

1. Social Security number;
2. Driver's license number or nondriver identification card number; or
3. Account number, or credit or debit card number, in combination with any required security code, access code, or password that 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 that compromises the security, confidentiality, or integrity of personal information maintained by the District. Good-faith acquisition of personal information by an officer, employee, or agent of (and 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 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

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:

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. Examples include, but are not limited to:
a. fraudulent accounts opened;
b. instances of identity theft reported; and/or
c. any other instance of identity or information theft.

4. Any other factors that 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 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. The District shall consult with the New York State Office of Cyber Security & 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 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) 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) 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:

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 individual;
2. Conspicuous posting on the 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 District shall notify the state attorney general, the Consumer Protection Board, and CSCIC 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 reprinting agencies will be furnished, upon request, by the Office of the State Attorney General.

*Adoption date:* January 4, 2012  
*Revised date:* September 18, 2019