No. 830

SECTION: OPERATIONS

TITLE: BREACH OF COMPUTERIZED PERSONAL INFORMATION

ADOPTED: March 21, 2007

REVISED:

SHALER AREA SCHOOL DISTRICT

830. BREACH OF COMPUTERIZED PERSONAL INFORMATION

1. Purpose	With the increased reliance upon electronic data, and the maintenance of personal information of students and employees in electronic format, the Board is concerned about the risk of a breach in the District's electronic system security and the possible disclosure of personal information. This policy addresses the manner in which the District will respond to unauthorized access and acquisition of computerized data that compromises the security and confidentiality of personal information.
2. Authority 73 P.S. Sec. 2301 et seq	The Board directs that District administrators shall provide appropriate notification of any computerized system security breach to any state resident whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed or acquired by unauthorized persons.
3. Definitions 73 P.S. Sec. 2302	**Breach of the system's security** – unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the District as part of the database of personal information regarding multiple individuals and that the District reasonably believes has caused or will cause loss or injury to any state resident. Good faith acquisition of personal information by an employee or agent of the School District for the purpose of the District is not a breach of the security of the system if the personal information is not used for a purpose other than the unlawful purpose of the District and is not subject to further unauthorized disclosure. **Individual** – means any natural person, not an entity or company.
73 P.S. Sec. 2302	**Personal information** – includes an individual's first initial and last name in combination with and linked to any one or more of the following, when not encrypted or redacted: 1. Social security number. 2. Driver's license number or state identification card number issued Instead of a driver's license.

3. Financial account number, credit or debit card number, in combination with any required social security code, access code, or password would permit access to an individual's financial account.

Pol. 801

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

Records – means any material, regardless of its physical form, on which information is recorded or preserved by any means, including written or spoken words, graphically depicted, printed, or electromagnetically transmitted. This term does not include publicly available directories including information that an individual has voluntarily consented to have publicly disseminated or listed, such as name, address, or telephone number.

4. Delegation of Responsibility
73 P.S. Sec. 2303

The Superintendent or designee shall ensure that the District provides notice of any system security breach, following discovery, to any state resident whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person. Such notice shall be made without a reasonable delay, except when a law enforcement agency determines and advises the District in writing that the notification would impede a criminal or civil investigation, or the District must take necessary measures to determine the scope of the breach and to restore the reasonable integrity of the data system. The District will also provide notice of breach if the encrypted information is accessed and acquired in an unencrypted form, if the security breach is linked to a breach of security of the encryption, or if the security breach involves a person with access to the encryption key.

73 P.S. Sec. 2302

The District shall provide notice by at least one (1) of the following methods:

1. Written notice to last known home address for the individual.

2. Telephone notice if the individual can be reasonably expected to receive the notice and the notice is given in a clear and conspicuous manner; describes the incident in general terms; verifies the personal information but does not require the individual to provide personal information; and provides a telephone number to call or Internet web site to visit for further information or assistance.

3. E-mail notice, if a prior business relationship exists and the School District has a valid e-mail address for the individual.

4. Substitute notice if the District determines that the cost of notice exceeds $100,000, the affected individuals exceed 175,000 people, or the District does not have sufficient contact information. Substitute notice shall consist of an email notice, conspicuous posting of the notice on the District's web site, and notification to major statewide media.

73 P.S. Sec. 2305
15 U.S.C. Sec. 1681a

If the District provides notification to more than 1,000 persons at one (1) time, the District shall also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and number of notices, without reasonable delay.

References:

Breach of Personal Information Notification Act – 73 P.S. Sec. 2301 et seq

Fair Credit Reporting Act – 15 U.S.C. Sec. 1681a

Board Policy – No. 801