Book	Policy Manual
Section	800 Operations
Title	~~Breach of Computerized Personal Information~~ **Security of Computerized Personal Information/Breach Notification**
Code	830

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.~~

The Board is committed to the security of the district's computerized data and to addressing the risk of a breach of the district's systems involving 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.

Authority

~~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.[1]~~

The Board requires that records containing personal information be securely maintained, stored and managed in compliance with state and federal laws, regulations, Board policy, administrative regulations and the district's Records Management Plan.[1][2][3][4][5][6][7][8]

The Board directs the district to provide notice as required by law to any resident of the Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed or acquired by unauthorized persons.[1]

Definitions

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 lawful purpose of the district and is not subject to further unauthorized disclosure.[9]

~~**Individual** - means any natural person, not an entity or company.~~[2]~~[3]~~

~~**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 security code, access code or password that would permit access to an individual's financial account.~~

~~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 containing information that an individual has voluntarily consented to have publicly disseminated or listed, such as name, address or telephone number.~~

Determination - a verification or reasonable certainty that a breach of the security of the system has occurred.[9]

Discovery - the knowledge of or reasonable suspicion that a breach of the security of the system has occurred.[9]

Encryption - the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.[9]

Personal information - includes an individual's first name or first initial and last name in combination with and linked to any one or more of the following, when not encrypted or redacted:[9]

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 security code, access code or password that would permit access to an individual's financial account.**
4. **Medical information, meaning any individually identifiable information contained in the individual's current or historical record of medical history or medical treatment or**

diagnosis created by a health care professional.[9]

5. **Health insurance information, meaning an individual's health insurance policy number or subscriber identification number in combination with access code or other medical information that permits misuse of an individual's health insurance benefits.**[9]

6. **A user name or email address, in combination with a password or security question and answer that would permit access to an online account.**

Personal information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.[9]**[10]**

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 containing information that an individual has voluntarily consented to have publicly disseminated or listed, such as name, address or telephone number.[9]

Redact - includes, but is not limited to, alteration or truncation such that no more than the last four (4) digits of a Social Security number, driver's license number, state identification card number or account number is accessible as part of the data.[9]

Delegation of Responsibility

~~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 the 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.[4]~~

~~The district shall provide notice by at least one (1) of the following methods:[2]~~

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 e-mail notice, conspicuous posting of the notice on the district's web site, and notification to major statewide media.~~

~~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 unreasonable delay.~~

The Superintendent or designee shall ensure that the district provides notice, as required by law, of any breach of the security of the district's systems.[1]

The Superintendent, in collaboration with appropriate administrators, shall develop administrative regulations to implement this policy, which shall include, but not be limited to:[1]

1. **Procedures following discovery of a breach.**

2. **Procedures for the determination of a breach and whether breach notification is required under the law.**

3. **Breach notification procedures including timeline requirements, who must be notified and methods for such notice.**

Guidelines

Upon determination of a breach of the security of the system, the Superintendent or designee shall provide notice to the district attorney in the county where the breach occurred and to any resident of the Commonwealth 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 in accordance with the provisions of law regarding timelines and methods of notification.[1]

The notice shall be made without an unreasonable delay, except when a law enforcement agency determines and advises the district in writing, citing the applicable section of law, 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.[11][12]

The district shall also provide notice of the 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.[1]

If a district service provider notifies the district of a breach regarding unencrypted and

unredacted personal information the district shall ensure the required notices outlined herein are provided.

Legal References

1. 73 P.S. 2305.1
2. 73 P.S. 2305.2
3. Pol. 800
4. 73 P.S. 2301 et seq
5. Pol. 830
6. Pol. 113.4
7. Pol. 216
8. Pol. 324
9. 73 P.S. 2302
10. Pol. 801
11. Pol. 828
12. Pol. 815
13. Pol. 317
14. Pol. 818
15. Pol. 916