LENAPE TECHNICAL SCHOOL

SECTION: OPERATIONS

TITLE: SECURITY OF COMPUTERIZED PERSONAL INFORMATION/ BREACH NOTIFICATION

ADOPTED: April 20, 2017

REVISED: June 15, 2023

	830. SECURITY OF COMPUTERIZED PERSONAL INFORMATION/BREACH NOTIFICATION
1. Purpose	The Joint Operating Committee is committed to the security of the school's computerized data and to addressing the risk of a breach of the school's systems involving the possible disclosure of personal information. This policy addresses the manner in which the school will respond to unauthorized access and acquisition of computerized data that compromises the security and confidentiality of personal information.
2. Authority	The Joint Operating Committee requires that records containing personal information be securely maintained, stored and managed in compliance with state and federal laws, regulations, Joint Operating Committee policy, administrative regulations and the school's Records Management Plan. [1][2][3][4][5][6][7][8] The Joint Operating Committee directs the school 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]
3. 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 school as part of a database of personal information regarding multiple individuals and that causes, or the school reasonably believes has caused, or will cause, loss or injury to any resident of the Commonwealth. Acquisition of personal information by an employee or agent acting in good faith on behalf of the school 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 school and is not subject to further unauthorized disclosure. [9] Determination – a verification or reasonable certainty that a breach of the security of the system has occurred. Discovery – the knowledge of or reasonable suspicion that a breach of the security of the system has occurred.

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 healthcare 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 username 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]

4. Delegation of Responsibility	The Administrative Director or designee shall ensure that the school provides notice, as required by law, of any breach of the security of the school's system. [1] The Administrative Director, in collaboration with appropriate staff, shall develop administrative regulations to implement this policy, which shall include, but not 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.
5. Guidelines	Upon determination of a breach of the security of the system, the Administrative Director 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 school in writing, citing the applicable section of law, that the notification would impede a criminal or civil investigation, or the school must take necessary measures to determine the scope of the breach and to restore the reasonable integrity of the data system [11][12] The school 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] **PSBA Revision 4/23 © 2023 PSBA** Legal References 1. 73 P.S. 2301 et seq 2. Pol. 113.3 3. Pol. 216 4. Pol. 324 5. Pol. 800 6. Pol. 800.1 7. Pol. 815 8. Pol. 830.1

	9. 73 P.S. 2302 10. Pol. 801 11. 73 P.S. 2303 12. 73 P.S. 2304 15 U.S.C. 1681a © PSBA 2023