NORTH ALLEGHENY SCHOOL DISTRICT

SECTION:	**OPERATIONS**
TITLE:	**BREACH OF COMPUTERIZED PERSONAL INFORMATION**
ADOPTED:	**JULY 19, 2017**
REVISED:	

830 - BREACH OF COMPUTERIZED PERSONAL INFORMATION

Section 1. Purpose

With the increased reliance upon electronic data, and the maintenance of personal information of students, and employees in electronic format, the Board acknowledges 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.

Section 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 individual or parent(s)/guardian(s) whose unencrypted and un-redacted personal information was or is reasonably believed to have been accessed or acquired by unauthorized persons.

Section 3. Definitions

73 P.S.
Sec. 2302

a. 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 individual. 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.

b. Individual - any natural person, not an entity or company.

73 P.S.
Sec. 2302

c. 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, date of birth, and/or address.
2. Health insurance information and insurance beneficiary information.
3. Student and/or staff medical records.
4. Gifted, 504 Plan, or IEP status.
5. Student assessment data.
6. Driver's license number or state identification card number issued instead of a driver's license.
7. 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.
8. Any other information deemed confidential in nature by the District.

Pol. 801

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

73 P.S. Sec. 2302

e. Records - 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.

Section 4. <u>Delegation of Responsibility</u>

a. The Superintendent or designee shall ensure that the District provides notice of any system security breach, following discovery, to any individual or parent(s)/guardian(s) 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.

b. 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.

73 P.S. Sec. 2302	c. If the District provides notification of a breach to more than 1,000 persons at one (1) time, the District must also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis (defined in the Fair Credit Reporting Act) of the timing, distribution, and number of notices. **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 – 801