No. 830

COMMONWEALTH CHARTER ACADEMY

SECTION: OPERATIONS

TITLE: BREACH OF COMPUTERIZED PERSONAL INFORMATION

ADOPTED: April 12, 2017

REVISED:

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 Commonwealth Charter Academy's electronic system security and the possible disclosure of personal information. This policy addresses the manner in which the CCA will respond to unauthorized access and acquisition of computerized data that compromises the security and confidentiality of personal information.

§ 2. Authority

73 P.S. § 2301, et seq.

The Board directs that CCA 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. § 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 CCA as part of the database of personal information regarding multiple individuals and that CCA reasonably believes has caused or will cause loss or injury to any state resident, CCA employee or student. Good faith acquisition of personal information by an employee or agent of CCA for the purpose of CCA 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 CCA and is not subject to further unauthorized disclosure.

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

73 P.S. § 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 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, telephone number, or e-mail address. § 4. <u>Delegation of Responsibility</u>
73 P.S. § 2303	The CEO or designee shall ensure that CCA provides notice of any system security breach, following discovery, to any state resident, employee or student 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 CCA in writing that the notification would impede a criminal or civil investigation, or CCA must take necessary measures to determine the scope of the breach and to restore the reasonable integrity of the data system. CCA 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. § 2302	CCA 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 CCA has a valid e-mail address for the individual. 4. Substitute notice if CCA determines that the cost of notice exceeds $100,000, the affected individuals exceed 175,000 people, or CCA does not have sufficient

	contact information. Substitute notice shall consist of an e-mail notice, conspicuous posting of the notice on CCA's web site, and notification to major statewide media.
73 P.S. § 2305 15 U.S.C. § 1681a	If CCA provides notification to more than 1,000 persons at one (1) time, CCA 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.
	References: Breach of Personal Information Notification Act – 73 P.S. § 2301, et seq. Fair Credit Reporting Act – 15 U.S.C. § 1681a