



Book	Policy Manual
Section	800 Operations
Title	Security of Computerized Personal Information / Breach Notification
Code	830- (Administrative Guideline Attachment)
Status	Active
Adopted	January 25, 2024
Last Revised	January 25, 2024

The District will take reasonable measures to maintain the security and confidentiality of personal information about staff, students, parents/guardians and District residents. The District will implement and maintain practices regarding physical, technical and administrative safeguards for both paper and electronic records.

Employees shall promptly report to the Superintendent or designee any security breach of the District's computerized data that compromises the security, confidentiality or integrity of personal information maintained by the District.

Identifying Security Breach

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized individual or an individual without valid authorization, the District will consider the following factors:

1. Whether the information is in the physical possession and control of an unauthorized individual, such as a lost or stolen computer or other device containing information.
2. Whether the information has been downloaded or copied.
3. Whether information was used by an unauthorized individual, such as fraudulent accounts or reported identity theft.
4. Other factors the District deems appropriate and relevant to such determination.

Determination of a Security Breach

A determination of a security breach means that there is a verification or reasonable certainty that a breach of the District's computerized data has occurred. Such a determination is made after a reasonable forensic investigation has been completed to determine the scope and nature of the incident and a legal determination is made that breach notifications are required.

The following individuals will generally be involved in making the determination that a security breach has occurred and that breach notifications are required, although additional individuals/consultants may be involved in making such a determination depending on the totality of the circumstances: (1) Superintendent; (2) Director of Technology; (3) Director of Business Affairs; (4) District Solicitor.

Procedure for Notification

If there is a legal determination that notification is required, notices of a breach of information security will be provided to the individuals whose unencrypted and unredacted personal information has been accessed or acquired by an unauthorized person.

The following steps will be taken by the employee designated to provide notification:

1. If the breach involved computerized data owned or licensed by the District, the District will directly notify those residents of the Commonwealth whose personal information was or is reasonably believed to have been accessed and acquired by a person without valid authorization.
2. If the breach involved computerized data maintained by the District, the District will directly notify the owner or licensee of the information of the breach immediately following discovery, if the personal information was or is reasonably believed to have been accessed and acquired by a person without valid authorization.
3. If there is a legal determination that notification is required, the notification to affected individuals will be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system. Notification will be provided within seven (7) business days of determination of the breach of the security of the system.
4. Notification will be provided to the District Attorney in the county where the breach of the security of the system occurred within three (3) business days following determination of the breach of the security of the system.
5. The required notification will include:
 - a. District contact information;
 - b. Description of the categories of information that were or are reasonably believed to have been accessed and acquired without authorization; and
 - c. Which specific elements of personal information were or are reasonably believed to have been accessed and acquired.

6. The notification requirement may be delayed if a law enforcement agency determines, and advises the District in writing, specifically citing 73 P.S. Sec. 2304, that such notification will impede a criminal or civil investigation. The required notification will then be made after the law enforcement agency determines that such notification does not compromise the investigation or national or homeland security.

The District will provide notice to affected individuals 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 website to visit for further information or assistance.
3. Email notice - if a prior business relationship exists and the District has a valid email address for the individual.
4. Electronic notice - if the notice directs the individual whose personal information has been materially compromised by breach of the security of the system to promptly change the individual's password and security question or answer, as applicable, or to take other steps appropriate to protect the individual's online account, and other online accounts that may use the same user name, email address and password or security question or answer, to the extent the District has sufficient contact information for the individual.
5. Substitute notice - if the District demonstrates one (1) of the following:
 - a. The cost of notice would exceed \$100,000.
 - b. The affected individuals exceed 175,000 people.
 - c. The District does not have sufficient contact information for the individual.

Substitute notice shall consist of an email notice, when the District has an email address for the individual; conspicuous posting of the notice on the District's website; and notification to major statewide media.

6. 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.

§