

Information Breach Notification Policy

This policy defines the circumstances under which the Patchogue-Medford Library shall provide notice regarding a breach in security of the Library's system that result in unauthorized access to private information.

Definitions

"Private Information" is personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:

1. Social security number
2. Driver's license number or non-drive identification card number; or
3. Account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account.

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

"Breach of the Security of the System" shall mean unauthorized acquisition or acquisition without valid authorization of computerized data which compromises the security, confidentiality, or integrity of Private Information maintained by the Library. Good faith acquisition of Private Information by an employee or agent of the Library for the purposes of the Library is not a Breach of the Security of the System, provided that the Private Information is not used or subject to unauthorized disclosure.

Investigation of Alleged Breaches of the Security of the System

Suspected or confirmed Breaches of the Security of the System must be reported immediately to the Director. The Director or designee will investigate all reports of Breaches of the Security of the System. In determining whether Private Information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, the Director or designee shall consider the following non-exhaustive list of factors:

- Indications that the Private Information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing Private Information; or
- Indications that the Private Information has been downloaded or copied; or
- Indications that the Private Information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

Notification

In the event the Director or designee determines or reasonably believes that Private Information has been acquired by an unauthorized person or a person without valid authorization, the Library shall send notifications to those affected by the breach, or those whose data may have been compromised, as well as to government officials as the Library deems appropriate, by at least one of the following methods:

- Written notice;
- Telephone notification provided that a log of each such notification is kept by the Library; or
- In cases where the Library determines that the cost of providing notice would exceed \$250,000, or that the affected class of subject persons to be notified exceeds 500,000, or that the Library does not have sufficient contact information, by Substitute Notice.

Substitute Notice shall consist of the following:

- E-mail notice when the Library has an e-mail address for the subject persons;
- Conspicuous posting of the notice on the Library's website; and
- Notification to major statewide media.

All notices provided under this Policy shall include contact information for the Library and a description of the categories of Private Information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification as to which elements of Private Information were, or reasonably believed to have been, improperly acquired.

Notwithstanding anything to the contrary, the Library may delay providing notification if a law enforcement agency determines that such notification impedes a criminal investigation. In such situations, notification need not be made until after such law enforcement agency determines that notification does not compromise its criminal investigation.

Adopted by the Board of Trustees: March 20, 2019