



## Information Breach Notification Policy

This policy defines the circumstances under which the Geneva Public Library (“the Library”) shall provide notice regarding a breach in security that results in unauthorized access to private information.

This policy applies to information stored by the Library. Suspected or confirmed information security breaches must be reported immediately to the Director. A breach is defined as unauthorized access to Library information. The Library will investigate all reports of breaches of security related to information maintained by the Library. Based on the results of the investigation, internal and/or external parties may be notified as necessary.

Upon notification of a suspected information security breach, the Library will:

- Report the breach to the appropriate officials;
- Block, mitigate, or de-escalate the breach, if possible;
- Implement processes and procedures to prevent similar breaches from occurring in the future.

### Internal Notification

The employee discovering the breach will report it to the Director who will establish an appropriate response strategy. If it is determined that criminal activity has taken place, the Director will notify law enforcement and the Library Board of Trustees President.

### External Notification

The Director will determine if external notification is required. External notification is required if any of the following conditions are met:

- Access has been gained to private information as that term is defined in [New York State Technology Law Section 208\(1\)\(a\)](#);
- A physical device that contains private information has been lost or stolen;
- There is evidence that private information has been copied or removed from a physical device containing sensitive information.

External notifications will go to anyone affected by the breach, or whose data may have been compromised, as well as to government officials, as required by law.

Adopted by the Board of Trustees: April 25, 2018