



## Information Breach Notification Policy

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

This policy applies to information stored by the Library. Suspected or confirmed information breaches must be reported immediately to the Executive Director.

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

- Investigate the breach and report it to the appropriate internal and/or external officials and parties;
- Block, mitigate, or de-escalate the breach, if possible;
- Implement processes and procedures to prevent similar breaches from occurring in the future.

### 1. Internal Notification

The employee who discovers the breach will report it to the Executive Director, who will establish an appropriate response strategy. If it is determined that criminal activity has taken place, the Executive Director will notify law enforcement, the President of the Board of Trustees (“the Board”), and the OWWL Library System.

### 2. External Notification

The Executive 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 § 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

**Amended by the Board of Trustees:** 3/30/2022, 3/29/2023, 3/27/2024

**Reviewed by the Policy Review Committee:** 3/11/2024