**Data Breach Notification Policy**

The following policy is adopted pursuant to §208 of the state Technology Law:

1. The following terms shall have the following meanings:
	1. “Private information” shall mean either:
		1. personal information consisting of any information in combination with any one or more of the following data elements, when either the data element or the combination of personal information plus the data element is not encrypted or encrypted with an encryption key that has also been accessed or acquired:
			1. social security number;
			2. driver's license number or non-driver identification card number;
			3. account number, credit or debit card number, in combination with any required security code, access code, password or other information which would permit access to an individual's financial account;
			4. account number, or credit or debit card number, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code, or password; or
			5. biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as fingerprint, voice print, or retina or iris image, or other unique physical representation or digital representation which are used to authenticate or ascertain the individual's identity; or
		2. a user name or e-mail address in combination with a password or security question and answer that would permit access to an online 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.

* 1. “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 personal information maintained by a state entity. Good faith acquisition of personal information by an employee or agent of a state entity for the purposes of the agency is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, such state entity may consider the following factors, among others:

* + 1. indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or
		2. indications that the information has been downloaded or copied; or
		3. indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.
	1. “Consumer reporting agency” shall mean any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports. A list of consumer reporting agencies shall be compiled by the state attorney general and furnished upon request to state entities required to make a notification under subdivision two of this section.
1. For any computerized data that includes private information that is owned or licensed by the Library, the Library shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any individual whose private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization. The disclosure shall 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 restore the integrity of the data system.
	1. Notice to affected persons is not required if the exposure of private information was an inadvertent disclosure by persons authorized to access private information, and the Library reasonably determines such exposure will not likely result in misuse of such information, or financial or emotional harm to the affected persons. Such a determination must be documented in writing and maintained for at least five years. If the incident affected over 500 residents of New York, the Library shall provide the written determination to the state attorney general within ten days after the determination.
	2. If notice of the breach of the security of the system is made to affected persons pursuant to the breach notification requirements under any of the laws listed in §208(2)(b)(i)-(iv) of the state Technology Law, additional notice to those affected persons is not required, but notice still shall be provided to the state attorney general, the department of state and the office of information technology services pursuant to §208(7)(a) and to consumer reporting agencies pursuant to §208(7)(b).
2. For any computerized data that includes private data that is maintained by the Library, but that the Library does not own, the Library shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization.
3. The notifications required may be delayed if a law enforcement agency determines that such notifications impede a criminal investigation. In that case, the required notifications shall be made after such law enforcement agency determines that such notifications do not compromise such investigation.
4. The required notifications shall be directly provided to the affected persons by written notice, or alternatively, by one of the methods set forth in §208(5)(b)-(d) of the state Technology Law.
5. Regardless of the method by which notice is provided, such notice shall include contact information for the Library, the telephone numbers and websites of the relevant state and federal agencies that provide information regarding security breach response and identity theft prevention and protection information, and a description of the categories of information that were, or are reasonably believed to have been, accessed or acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so accessed or acquired.
	1. The relevant state agencies include:
		1. Office of the State Attorney General
		2. Department of State
		3. State Office of Information Technology Services
	2. The relevant federal agencies may include:
		1. Department of Homeland Security
		2. The Federal Bureau of Investigation (FBI) Internet Crime Complaint Center
		3. Cyber and Infrastructure Security Agency
		4. Federal Trade Commission
		5. Federal Communications Commission
		6. Department of Health and Human Services
6. a. In the event that any New York residents are to be notified, the Library shall notify the state attorney general, the department of state and the state office of information technology services as to the timing, content and distribution of the notices and approximate number of affected persons and provide a copy of the template of the notice sent to affected persons. Such notice shall be made without delaying notice to affected New York residents.
7. In the event that more than 5,000 New York residents are to be notified at one time, the Library shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.
8. Whenever notification of a data breach must be provided to the Secretary of the federal Department of Health and Human Services (HHS), then notification of the breach should also be given to the attorney general within five business days of notifying HHS.

***Policy adopted by the Liberty Public Library Board of Trustees on Feb. 25, 2025***