Cybersecurity

It is the intention of the Staff and Board of Trustees of the North Babylon Public Library to maintain a solid program of network security and to review this policy on a regular basis in order to accomplish the following:

1. Recognize and analyze the risks/threats to electronic resources
2. Determine which risks/threats are most likely to occur
3. Apply best practices to protect against these risks/threats
4. Maintain backup for sensitive files
5. Regularly review security alerts and bulletins regarding new vulnerabilities
6. Insure privacy guidelines

It should be clear that this policy addresses broad knowledge and understanding rather than specific actions since this field changes so frequently.

The Library's administration is responsible for implementing a secure technology infrastructure using appropriate vendors and products. All staff members are responsible for protection of technology and informational assets of the Library, which must be protected from unauthorized access, theft and destruction. This includes: devices/hardware, software and files/data. The library reserves the right to examine/monitor any or all computer systems/devices under its control as deemed necessary to ensure the security of such systems, or in the event of a breach, to enable forensic efforts to be instituted.

Business Office Computers: are the most critical, based on the sensitivity of the data stored on them (payroll, fund accounting data, banking, health insurance, personnel records, etc.). These computers are secured with passwords and are backed up to a physical flash drive kept by the Senior Account Clerk off-site and saved to a back-up hard drive. Other back-up services and solutions continue to be investigated. This computer will be maintained on a UPS. The Library will continue to keep abreast of industry standards applicable to public libraries.

Local Area Network: also critical. Located in separate room with additional ventilation. No access to staff other than Computer Tech and Library Director without prior authorization. The LAN will be maintained on a UPS.

Other Staff Computers: will be backed up by the individual users (either USB or Shared Network Drive); assistance is available from the Computer Tech. It has been suggested that a good back-up will render an infected computer dispensable.

Public Computers: no back up is made by staff, data must be saved to a user's personal USB stick. Monitors face library staff, no privacy is implied.

Assigned Accounts: individually assigned Library computer and Office365 accounts to staff will be deleted upon departure from the library.

Patron Data: held on site are predominantly library card applications and patron photographs. Although not cybersecurity issues, this information will be kept confidential.

PALS: the Integrated Library System used by the Libraries of Suffolk County (Innovate Interfaces) is maintained by the Suffolk Cooperative Library System. All PALS records are handled by SCLS. This includes maintenance, back-ups,

upgrades, etc. Information derived from the PALS database will be kept confidential.

Computer Tech: monitors equipment and assists staff and patrons with technology issues. Library staff and patrons may not install software on library computers or other devices without authorization from both the Computer Tech and Library Director. The Computer Tech will operate security tools, malware prevention devices, etc. on Library computers/devices. Anti-virus/anti-malware/etc. software is used to prevent everyday threats. When necessary, removal tools are used to clean and scan the PC in question are used. As threats evolve, security tools evolve. It is the responsibility of the Computer Tech to remain at the forefront of expertise on cybersecurity issues.

Wireless Network: the public wireless network is separate from the hardwired staff network. It is subject to the same level of precautions as any other Library network.

Approved by the Board of Trustees
September 18, 2017