Towanda District Library Cyber Security Policy

The technology and information assets of the Towanda District Library are made up of the following components:

- Devices (including, but not limited to CPUs, discs, servers, PC systems, tablets, printers, etc.)
- Computer software (including, but not limited to Operating Systems, Office productivity suites, drivers, web browsers, email clients, mobile apps, etc.)
- Files and Data (including, but not limited to Word documents, Excel spreadsheets, payroll data, login credentials, digitally-stored patron information, etc.)

As such, a system of classification will be maintained, whereby the most sensitive information is subject to more stringent security measures than less sensitive information. The Library reserves the right to examine, or monitor any or all computer systems and devices under its control as deemed necessary to ensure for the Library the security of such systems, or in the event of a breach, to enable forensic efforts to be instituted.

Integrated Library System (ILS) -This network is defined as the collective telecommunications and hardware facilities, including, but not limited to, high speed data circuits, routers, and switches that communicate for the purpose of the transmission of data required to operate and provide intranet and internet service. Use of this network is subject to the following conditions:

- Equipment placed in the Towanda District Library (TDL) remains the property of TDL. At any time, TDL may modify, replace, upgrade or remove for repair any of these devices. TDL will attempt to do so without any interruption of services.
- No third-party hardware, software or service, including but not limited to local area networks, wireless networks, or hardware or software, may in any way be connected to or interfaced with TDL equipment or the data network, either temporarily or permanently, without the express written approval of the TDL Director or its Executive Board.
- TDL is not responsible for installation, troubleshooting, or support of any third party hardware, software or service except for such services offered by TDL as part of its service program and as previously approved by TDL.
- TDL employees must use the equipment, network, and databases solely for library or patron business.

Adopted September 20, 2022

- TDL reserves the right to monitor the use of its equipment, network, and database and to have access to its equipment placed in the library.
- TDL employees and board of trustees using TDL equipment, network, and database should not do so with any expectation of privacy. By the use of such equipment, network or database, users waive any and all rights to privacy.
- Confidential library records must be handled in accordance with all applicable local, state, and federal statutes and regulations.
- All passwords to the TDL online accounts must be protected and not supplied to individuals other than library employees and board trustees. These passwords will be kept with the Director and a trustee appointed by the Board of Trustees and any updates will be shared with both parties.
- Any online financial passwords will not be shared.

Adopted September 20, 2022