Dansville Public Library

200 Main Street Dansville, NY 14437
585-335-6720 | Fax: 585-335-6133
dansvillelibrary.org
Where knowledge grows

ONLINE BANKING AND WIRE TRANSFER POLICY

PURPOSE

This policy establishes the rules governing the library's use of online banking and wire transfers. It protects public funds by ensuring that electronic financial transactions are authorized, documented, and subject to appropriate oversight. This policy applies to the board of trustees, the director, the treasurer, and any staff member with access to the library's online banking accounts.

This policy does not govern credit and debit card acceptance, online payment processing, or remote deposit capture. Those activities are addressed in separate policies.

AUTHORIZED TRANSACTIONS

The library uses online banking for the following purposes:

- Reviewing account balances and transaction activity
- Transferring funds between library accounts
- Initiating payments to authorized vendors
- Initiating wire transfers for bond payments, investment transactions, or other large-dollar settlements as authorized by the board

Any transaction type not listed above requires prior board authorization before it may be conducted through online banking.

AUTHORIZED USERS

The board designates the following positions as authorized to access the library's online banking accounts:

- Treasurer
- Board President
- Library Director (view-only access for oversight purposes)
- Accounting Consultant designated during the annual organizational meeting (view-only access)

The Library Director maintains a current list of individuals in each authorized position. The board reviews and confirms this list annually during their annual organizational meeting or whenever a personnel change affects access.

No other third-party vendor, bookkeeper, payroll processor, or consultant may have direct access to the library's online banking accounts. Vendors receive payment through the library's normal claims and warrant process after board audit and approval.

SEGREGATION OF DUTIES

At least two individuals must be involved in each electronic transaction. Specifically:

- The person who initiates a transaction may not also authorize it.
- The person who authorizes a transaction may not also record it in the library's financial records.
- No individual may both prepare a disbursement and audit or approve the underlying claim.

Dansville Public Library

200 Main Street Dansville, NY 14437
585-335-6720 | Fax: 585-335-6133
dansvillelibrary.org
Where knowledge grows

WIRE TRANSFERS

Before the library conducts any wire transfer, the board enters into a written agreement with the depository bank. That agreement must, consistent with New York General Municipal Law Section 5-a, identify the accounts from which wire transfers may be made, identify the officer or officers authorized to order a transfer, specify the manner in which transfers will be made, and implement a security procedure as required by Uniform Commercial Code Section 4-A-201.

No individual may execute a wire transfer without written or documented authorization from the treasurer or their designated deputy. The authorization and transmitting functions are always performed by different individuals.

Wire transfers are used only for:

- Bond payments or debt service
- Investment transactions
- Other large-dollar settlements expressly authorized by the board

The depository bank must provide written confirmation of each wire transfer to the authorizing officer no later than the next business day following the transfer.

The library instructs its depository bank to require a callback confirmation from a designated individual other than the person who initiated the transfer before executing any wire transfer. The library may also direct its bank to block wire transfers to foreign accounts or to any institution other than authorized counterparties.

Because wire transfers do not pass through the normal accounts payable cycle, the Library Director ensures that each transfer is captured in the accounting records promptly and supported by documentation showing the purpose, amount, source account, and destination account.

CLAIMS AND BOARD REPORTING

All electronic disbursements, wire transfers, and online transaction fees appear on the warrant submitted to the board for monthly approval. Staff may not exclude transactions from the warrant because they lack a check number. The board reviews a detailed transaction listing, not a single lump-sum total.

Each transaction must be supported by documentation and approved by the board before or, where timing requires, promptly after the disbursement occurs.

PASSWORD AND ACCESS CONTROLS

Each authorized user has a unique username and password. Sharing credentials is prohibited. The library treats credential sharing as a serious internal control failure because it makes it impossible to determine who initiated any specific transaction.

Passwords must meet complexity requirements: a minimum of eight characters, including at least one uppercase letter, one lowercase character, one number, and one special character. Passwords may not include easily guessed words or names.

The library changes passwords and reviews access rights whenever an authorized user leaves their position, changes roles, or is no longer authorized to access online banking. The Library Director is responsible for ensuring that departing employees are promptly removed from all banking access.

Authorized users may not save banking usernames or passwords in a web browser and may not access the library's online banking from a public computer or an unprotected mobile device. Users type the bank's website address directly into the browser rather than following a link from an email or search engine result.

SECURITY PRACTICES

The library uses multi-factor authentication (also called two-factor authentication) for all online banking access where the bank makes it available. Multi-factor authentication requires the user to verify their identity using at least two methods: something they know, such as a password; something they have, such as a phone or token; or something they are, such as a fingerprint.

The director ensures that computers used for online banking:

- Have current antivirus, anti-spyware, and malware protection installed and updated
- Have operating system and software security patches applied promptly
- Use a wired rather than wireless network connection for financial transactions where possible
- Are logged out of all banking sessions completely when the session ends, not merely closed

The library works with its insurance provider to maintain coverage appropriate for cyberfraud risks, including fraudulent transfers and data breaches.

Staff with online banking access receive training at least annually on safe computing practices. Training covers recognizing phishing emails and social engineering schemes, avoiding untrusted links and attachments, and verifying the legitimacy of unexpected requests involving financial transactions. The Library Director documents completion of this training.

BANK AGREEMENTS AND SIGNATURE CARDS

The board confirms that its signature card agreements with all depository banks are consistent with this policy. If this policy requires two authorizations for disbursements, the bank signature card must reflect that requirement. A signature card that allows one-signature disbursement when this policy requires two removes a critical control.

REVIEW

The board reviews this policy every five years, consistent with 8 NYCRR § 90.2, or sooner if a significant change in law, technology, or library operations warrants an earlier review.

Approved by the Dansville Public Library Board of Trustees on 6/8/2026