PERSONNEL
Confidentiality of Library Records

I. **STATEMENT** The Red Jacket Community Library (Library) is committed to protecting patron privacy, patrons right to access information, and the confidentiality and security of the personally identifiable information (PII) collected and stored by the Library and the OWWL Library System (OWWL).

II. **PURPOSE** To uphold the OWWL Systems Access and Confidentiality of Library Records Policy, establish practices for employees authorized to access the OWWL Information System as necessary for their job functions, and to maintain the security of patron PII collected by the Library.

III. **POLICY**

A. USER RECORD CONFIDENTIALITY

1. The Library acknowledges its responsibility under New York State Civil Practice Law & Rules § 4509 to maintain the confidentiality of library records which contain the names or PII of library users.
    a. New York statutes protect the privacy rights of library users and prohibits the release of library records, including but not limited to records related to the circulation of library materials, computer database searches, interlibrary loan transactions, reference queries, requests for photocopies of library materials, title reserve requests, or the use of audio-visual materials, films, or records.
    b. Library records may be consulted and used by library staff to the extent necessary for the proper operation of the Library.
    c. Library records must not be disclosed except upon request or consent of the user or pursuant to subpoena, court order or where otherwise required by statute with the advice of legal counsel.
2. Librarians, library staff, and library volunteers are prohibited from disclosing any patron PII or any confidential library records.
    a. Examples of practices that must be avoided because they would constitute a breach of library record confidentiality and demonstrate a violation of this policy.
    b. Tell a third party whether a person has a library card.
    c. Write the name of a borrower on a book card which is placed in the book.
    d. Tell a parent what their child has borrowed, even if the borrowed item is overdue.
    e. Send a reserve notice or overdue reminder on a postcard which reveals the title of the item.
    f. Reveal the nature of a user's reference question to another person.
    g. Reveal a user's attendance at the Library.
3. This confidentiality law makes clear that a user's library use habits are strictly private; there are no exceptions. This law applies to all libraries in the state of New York.

B. USER RECORDS AND PATRON PII

1. Library patron PII is general data about a library user. Examples include name, address, e-mail address, telephone number, and date of birth, either alone or in combination.
2. Additional patron information, data about user activity that can be tied back to a user, includes circulation history, hold requests, or paid bills. These data are collected and stored in the OWWL Information System and are considered confidential information.
3. For the purposes of this policy, the term "patron PII" describes all confidential information about a user whether it is traditionally considered PII or not.

C. PATRON CONSENT

1. When completing a library card application at the Library, the patron consents for their data to be used for automated library notifications regarding available holds, checkouts, renewals, overdue materials, and card expirations.
2. Patrons should be aware that notifications of item availability or fines by e-mail or text message will include the title of the item.
3. Libraries may also directly communicate with a patron about issues with their account. No other access is assumed or approved when registering for a library card.

D. OWWL SYSTEMS ACCESS RESTRICTIONS

1. Local patron opt-in does not authorize the Library to use data stored in the Integrated Library System (ILS) or any other OWWL provided information systems.
2. Patron PII should never be exported from any of the OWWL Information Systems for the purpose of being shared with or uploaded to any third-party or third-party services.
    a. Examples of third parties include, but are not limited to, individuals not employed by the Library, outside ad or survey firms, Friends groups, and foundations.
    b. Examples of third-party services include, but are not limited to, fundraising platforms, Dropbox, and Google Drive.

E. ACCESSING THE OWWL INFORMATION SYSTEM

1. For electronic security purposes only devices meeting all the following requirements shall be used to access the ILS or the OWWL reporting tool with staff credentials.
    a. The device must be library owned.
    b. The device must be designated only for staff use (i.e., should not be lent to the public).
    c. The device must have an up-to-date operating system.
    d. The device must have up-to-date virus protection.
    e. The device must have an up-to-date web browser.
2. No file containing patron PII should be downloaded to or stored on a personal device. Files include, but are not limited to:
    a. Files generated by the ILS.

b. Files transmitted via email.

c. Files accessed on the OWWL reporting tool.

3. Any PII accessed on a device must be subsequently deleted.

4. When using shared computers or browsers, staff must avoid saving login credentials (usernames and passwords) used to access System Information Systems to a browser's password manager.

5. Electronic devices should be locked or logged out of when not in use or when a staff user is not at (or within immediate line of sight of) the workstation.

6. Devices on which patron PII is stored or accessed should be properly secured against unauthorized access.

a. Only library staff members are authorized to access System Information Systems (i.e. Evergreen and email services).

F. MANAGEMENT OF FILES, REPORTS, AND DOCUMENTS CONTAINING PATRON PII

1. Best practices for handling files, reports, and/or documents containing patron PII include, but are not limited to:

a. Accessing files or any links to files only on library-owned equipment.

b. Avoid using personally owned computers, mobile devices, and services, like Dropbox, to access, save, or store files.

c. Ensure that files and printed copies are kept secure from unauthorized access.

d. Avoiding transmitting files using methods that may not be secure, such as by e-mail attachment.

e. Instead, transmit files by using a shared drive on your local network or library-owned removable media like a flash drive.

f. Avoiding sharing files with, or uploading files to, unauthorized third-parties or third-party services.

g. Deleting files and emptying the recycling bin/trash when you are done with them.

h. Shredding any printed copies when you are done with them.

G. PII COLLECTION, STORAGE, AND USE

1. PII is collected and stored in the OWWL Information Systems and is considered confidential.

2. The Library collects the minimum PII necessary to conduct library-related business, the administration of library services, and to assist the specific person to whom the information pertains.

3. Only data necessary to provide library services should be collected and stored in the ILS.

a. Examples of data appropriate for collection include, but are not limited to name, address, e-mail address, telephone number, and date of birth.

b. Examples of data inappropriate for collection include, but are not limited to health information, and driver's license number.

4. Data about patrons should only be stored in the System Information Systems for the length of time necessary for operational or legal purposes.

   a. As soon as a borrowed item is returned to the library the borrowing history linked to that item is deleted from the user's record.

   b. However, the name of the last user who borrowed the item in addition to the name of the current borrower of the item are both retained by the software in the item's record.

   c. In addition, if a fine is owed or an outstanding bill exists, that information stays on the user record until after payment has been received.

   d. The software also retains information on pending requests for items requested by a user.

5. Patron PII should be used only for providing library services, such as automated library notifications regarding available holds, checkouts, renewals, overdue materials, and card expirations.

   a. Libraries may also directly communicate with a patron about issues with their account.

   b. No other access is assumed or approved when accessing PII.

6. As a member of OWWL, the Library maintains certain administrative information regarding the use of the OWWL Information System and managed computer services accessed by individuals through member libraries or via remote access. This information is kept for administrative purposes only.

H. REQUESTS FOR INFORMATION FROM AN AGENCY OR INDIVIDUAL

1. Only the Library Director, or Director's designee, is authorized to respond to any form of judicial process or to provide any patron-specific or library-business information, in writing or in oral form, to a law enforcement officer or other person.

2. No user PII or library transactions may be divulged to third parties except by court order.

3. In the event a Library staff person is requested to provide patron information to any outside agency or individual, the following procedures must be followed:

   a. The staff member receiving the request to examine or obtain information relating to circulation, computer activity or other records identifying the names of Library users, will immediately ask for identification, then refer the person making the request to the Director or designee, in the Director's absence, who shall explain the Library's confidentiality policy. The staff member will not disclose any information.

   b. The Director, upon receipt of a process, order, or subpoena, shall contact the OWWL Executive Director and consult with legal counsel to determine if such process, order, or subpoena is in good form and if there is a showing of good cause for its issuance.

   c. If the process, order, or subpoena is not in proper form or if good cause has not been shown, insistence shall be made that such defects be corrected before any records are released. Without documents in proper form, law enforcement has no authority to compel disclosure of any information, other than the name of the person speaking to law enforcement officers.

d. Any threats or unauthorized demands (i.e., those not supported by a process, order, or subpoena) concerning circulation, computer or other records identifying the names of library users shall be reported to the Director immediately.

e. If the document is a search warrant that authorizes immediate search and seizure, the staff member will inform the officer that the Library Director and legal counsel will be contacted immediately and request the patience of the officer. (The officer may inform the staff member that the warrant is "secret." This does not preclude notification of the Director and legal counsel.) If the officer declines to wait, the staff member should:

f. Carefully inspect the warrant and monitor the search.

g. Retain a copy of the warrant and request an inventory of the materials in question. Offer the officer a copy of any data requested.

h. At the conclusion of the search, immediately make a written record of all events that transpired.

i. Add the copy of the warrant, requested documents to the written record of the event and place it in a secure location such as the Library safe.

4. In the event the staff member is requested to provide patron information to any outside agency or individual the following procedures must be followed:

I. INFORMATION SECURITY BREACH NOTIFICATION

1. Upon notification of a suspected security breach of "private information" as defined in NYS Technology Law § 208, the Library must:

   a. Report the breach to the appropriate officials.

   b. Block, mitigate, or de-escalate the breach, if possible.

   c. Implement processes and procedures to prevent similar breaches from occurring in the future.

2. Internal Notification

   a. The person/department discovering the breach must report it to the Network Administrator (OWWL Library System IT Department) and to the Library Director and must work with them to establish an appropriate response strategy.

   b. If the Library's investigation determines that criminal activity has taken place, the Director must notify the Board of Trustees.

3. External Notification

   a. The Network Administrator, in consultation with the Library Director, must determine if external notification is required.

   b. External notification is required if any of the following conditions are met:

      i. Unauthorized access has been gained to sensitive information.
      ii. A physical device that contains sensitive information has been lost or stolen.
      iii. There is evidence that sensitive information has been copied or removed from a physical device.

c. 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.

J. EMPLOYEE CONFIDENTIALITY AGREEMENT

1. To access information stored by the Library and OWWL information systems, all Library employees are required to read the Confidentiality of Library Records Policy and agree to its contents.

   a. Employee agreement indicates their understanding that access to these systems, manual and automated, containing PII and other Library records information is limited to the requirements of their job duties, and such information is not to be disclosed to unauthorized persons.

2. The Library provides annual staff training and collects annual agreements from employees using the Confidentiality Agreement form (Appendix M).

K. BOARD RESPONSIBILITY

1. The Board of Trustees is responsible to uphold this policy and establish appropriate local controls to prevent infraction of this policy and the OWWL Systems Access and Confidentiality of Library Records Policy.

IV. REFERENCES

A. Library records. NY CIVIL PRACTICE LAW & RULES § 4509 (2023).

B. Notification; persons without valid authorization has acquired private information. NY STATE TECHNOLOGY LAW § 208 (2023).

	Revision History
2/20/2024	Aligned with OWWL System Access and Confidentiality of Library Records Policy
11/16/2020	Added section on Information Security Breach Notification