PERSONNEL
Confidentiality of Library Records

I. STATEMENT: The Red Jacket Community Library (RJCL) is committed to protecting patron confidentiality, including the borrowing information of patrons, and their right to access information that is controversial, sensitive or personal.

II. PURPOSE To provide guidelines to the library staff to ensure that patrons' library use habits are strictly private.

III. POLICY:

A. The RJCL acknowledges its responsibility under New York State Civil Practice Law & Rules, Section 4509 to maintain the confidentiality of library records which contain the names or other personally identifying information (PII) regarding the users of our member libraries. Such information shall not be disclosed except as specified in law and with the advisement of the Library's legal counsel.

B. New York State Law guarantees the confidentiality of library patron borrowing records. Library records relating to an individual patron's use of the library and its resources are confidential. These records may be consulted and used by library staff in the course of carrying out library operations, but will not be disclosed to others except upon the request or consent of the library user, or pursuant to subpoena, court order, or otherwise required by law.

New York State Civil Practice Law and Rules § 4509: Library records
Library records, which contain names or other personally identifying details regarding the users of public, free association, school, college and university libraries and library systems of this state, 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, shall be confidential and shall not be disclosed except that such records may be disclosed to the extent necessary for the proper operation of such library and shall be disclosed upon request or consent of the user or pursuant to subpoena, court order or where otherwise required by statute.

1. **Explanation:** The New York State Confidentiality Law protects the privacy rights of library users. This law prohibits the release of any information relating the name of a person and his/her library use without a properly executed subpoena from a court of law. Under this law, librarians, staff, volunteers, and board members cannot:
    a. Tell a third party whether a person has a library card.
    b. Write the name of a borrower on a book card which is placed in the book.
    c. Tell a parent what his/her child has borrowed, even if it is overdue.
    d. Send a reserve notice or overdue reminder on a postcard which reveals the title of the item.
    e. Reveal the nature of someone's reference question to another person.
    f. Reveal a patron's attendance at the library.
2. This law makes it quite clear that a person's library use habits are strictly private; there are no exceptions. It applies to every library in the state.

C. The USA PATRIOT ACT also requires presentation of a subpoena for access to patron records.

D. PERSONALLY IDENTIFYING INFORMATION (PII) COLLECTED

1. The RJCL collects the minimum personally identifying information necessary to conduct library-related business, including the circulation of library materials, contacting library patrons regarding library transactions and services, and connecting to third-party services that support library services.
2. As a member of the Pioneer Library System (PLS), RJCL maintains certain administrative information regarding the use of PLS information systems and managed computer services accessed by individuals through member libraries or via remote access. This information is kept for administrative purposes only.
3. RJCL patron records and sharing: The information in a RJCL patron record is the property of the Library. While other PLS libraries may have access to that data, no other library can use that data for anything other than library transactions. RJCL can use the data for library mailings. We may also allow the Friends of the Red Jacket Community Library to use the patron data. Information will not be given to any other organization. Patrons who do not wish to have their name, address, email and telephone shared with the Friends of the Red Jacket Community Library should notify the Library to have their information removed from that list.
4. Borrowing history. As soon as an item is returned, the link to that item is deleted from the patron record. However, the software retains in the item's record, the name of the last person who took it out, and the name of the current borrower of the item. In addition, if a fine is owed or an outstanding bill exists, that information stays on the patron record until after payment has been received. The software also keeps the track of items when a patron has a pending request for an item.
5. Email and text message notices. Patrons who wish to be notified of item availability or fine notices by e-mail or text message should be aware that the message will include the title of the item.

E. EMPLOYEE CONFIDENTIALITY AGREEMENT

1. All Red Jacket Community Library staff, in order to have access to RJCL information systems, are required to read this Confidentiality of Library Records Policy and agree to its contents. Agreement indicates their understanding that access to these systems, manual and automated, containing PII and other library record data is limited to the requirements of their job, and such information is not to be disclosed to unauthorized persons.
2. RJCL provides annual staff training and collects agreements from staff using the Confidentiality Agreement form (Appendix).

F. REQUESTS FOR INFORMATION FROM LAW ENFORCEMENT AGENCIES

1. No RJCL staff other than the 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 individual data or transactions may be divulged to third parties except by court order.
3. In the event a RJCL 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 institution's confidentiality policy. The staff member will not disclose any information.

b. The Director, upon receipt of a process, order, or subpoena, shall 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. The Director should contact the PLS Executive Director.

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:

(1) Carefully inspect the warrant and monitor the search.

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

(3) At the conclusion of the search, immediately make a written record of all events that transpired. Add the copy of the warrant, request documents, and the written record of the event to the Library's incidents file.

G. INFORMATION SECURITY BREACH NOTIFICATION

1. Upon notification of a suspected security breach of "private information" as defined in NYS Technology Law § 208 (see References), 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 (Pioneer 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:

      (1) Access has been gained to sensitive information

      (2) A physical device that contains sensitive information has been lost or stolen

      (3) There is evidence that sensitive information has been copied or removed from a physical device containing sensitive

   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.

IV. REFERENCES

A. Under NYS Technology Law § 208 (https://its.ny.gov/nys-technology-law), "Private information" shall mean either:

(i) 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 to 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

(ii) 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.

Revision History	
Oct 2020	Added section on Information Security Breach Notification