

# Racine Public Library

## Confidentiality and Privacy Policy

### Privacy Statement

Protecting Library user privacy and keeping confidential information that identifies individuals or associates individuals with their use of Library books, materials, equipment, programs, services, facilities, and/or staff assistance is an important principle of the Library. This policy affirms the Library's commitment to privacy, explains the information that the Library collects, and alerts visitors to Library facilities and users of remotely accessed Library services of the privacy choices available to them.

### Definition of Terms

- **Privacy** is the right to seek information through Library resources without having the subject of interest known or examined by others.
- **Confidentiality** exists when the Library possesses personally identifiable information and keeps that information private on the patron's behalf.
- **Personally identifiable information** is information such as name, Library card number, e-mail or mailing address, telephone number, or any financial information relating to a patron and his or her accounts.

### Legal Protections and Exceptions

Wisconsin law has strong protections in place to assist the Library in keeping records confidential. In certain circumstances, Library records may be subject to disclosure to law enforcement officials under provisions of state law or federal law under the provisions of the USA Patriot Act (Public Law 107-56). In accordance with the USA Patriot Act, public libraries must allow an immediate search and possible seizure of equipment or information if presented with a FBI National Security Letter or Foreign Intelligence Surveillance Act Warrant. Staff members are provided training in handling requests from law enforcement. The staff procedure can be found in Appendix 1 to this policy.

The relevant Wisconsin laws concerning the confidentiality of Library records are Wisconsin Statutes Section 43.30 and the Wisconsin Personal Information Practices Act (Sections 19.62 to 19.80). Library records include any record of use of Library materials, resources, or services.

Wis. State Statute 43.30 requires that Library records may only be disclosed under the following circumstances:

1. With the consent of the individual Library user.
2. To a custodial parent or legal guardian of a juvenile under 16 years of age.
3. By court order.

4. Upon the request of a law enforcement officer who is investigating criminal conduct alleged to have occurred at the Library. In this instance, the Library shall disclose all records pertinent to the alleged criminal conduct that were produced by a surveillance device under the control of the Library.
5. To persons acting within the scope of their duties in the administration of the Library or Library system.
6. To other libraries for interlibrary loan purposes in accordance with the standards set forth in Wisconsin Statute Sections 43.30(2) and (3).
7. To a qualifying third party<sup>1</sup> to assist with delinquent accounts. Under the provisions of the law, the Library may only disclose the individual's name, contact information and the quantity, types and value of unreturned materials, not the titles of the items.

## **Library Records**

The Library avoids creating unnecessary records and retaining records longer than needed for Library business purposes.

1. To receive a Library card, Library users are required to provide identifying information such as name, birth date, picture ID, and physical as well as mailing address (if different). The identifying information is retained, as long as the Library user continues to use the Library card. In most cases the information will be in the database for a maximum of three years after the person stops using the Library card at which time the record is deleted.
2. A Library user's circulation record includes current identifying information, items currently checked out<sup>2</sup> or on hold, as well as overdue materials and fines.
3. Ninety days after an item is returned, the Library System removes the information regarding the last patron to check it out which deletes the patron from the item history log. If the item had associated fines, the fine transactions are saved.
4. The Library may also gather information necessary to provide a requested service to a Library user including but not limited to the following examples:
  - Records of electronic access information such as the Library card or guest pass number used to log onto Library public computers or search a Library database
  - Records for interlibrary loan requests or reference services
  - Records needed to sign up for or participate in Library classes and programs

- Records for use of meeting rooms
- Records for receiving emails and/or text messages about Library services and programs

Once there is no longer a need for the information, personally identifying records are destroyed. Emails sent to Library staff may be subject to open records requirements.

5. The Library treats records as confidential in accordance with Wisconsin State Statute (43.30). The Library will not collect or retain private and personally identifiable information without the person's consent. If consent to provide personally identifiable information is given, the Library will keep it confidential and will not sell, license or disclose it to any third party, except for purposes described by the law.

## **Access to Accounts and Patron Responsibility**

### **Protecting a Patron Account**

It is the patron's responsibility to notify the Library immediately if a Library card is lost or stolen or if he or she believes someone is using the card or card number without permission. The Library recommends these precautions:

- Log off systems after use
- Don't share the Library card, user IDs, or passwords
- Select passwords which are easy to remember, but difficult for others to guess by including a mixture of numbers, symbols, and/or upper and lowercase letters

### **Keeping Account Information Up-To-Date**

A patron may access his/her personally identifiable information held by the Library and is responsible for keeping the information accurate and up-to-date. The purpose of accessing and updating personally identifiable information is to ensure that Library operations can function properly. A patron may view or update his/her personal information in person. He or she may be asked to provide some sort of verification or identification card to ensure verification of identity.

### **Parents and Children**

For the protection of patrons, parents seeking records of their minor child, under age 16, may be asked to provide proof of their child's age as well as evidence they are the custodial parent. According to Wisconsin State Statute 3.30(1b)(1a) "Custodial parent" includes any parent other than a parent who has been denied periods of physical placement with a child under s.767.41(4).

### **Items on hold**

Items placed on hold for Library patrons are shelved for pick-up in the public areas of the Library. Patrons of any age may choose to have other people pick up their holds. Holds will be checked out on the Library card presented at the time of check-out.

## **Public Computer Use and the Library's Automation Systems**

The Library routinely and regularly purges information that may be linked to Library users, such as information from web servers, mail servers, computer time management software, interlibrary loan requests, and other Library information gathered or stored in electronic format.

The Library System maintains the online catalog and a number of databases. The Library System automatically collects and maintains statistical information about Library users' visits to the Library catalog and databases. This information includes the IP address of the visitor, the computer and web browser type, the pages used, the time and date, and any errors that occurred. This information is used for internal reporting purposes and individual users are not identified.

Network traffic is monitored to identify unauthorized attempts to upload or otherwise damage the web service. If a Library user chooses to pay fines and fees via credit card, the credit card number is not stored in the user's Library account; it is simply passed through to the payment processor.

## **Websites**

The Library's website contains links to other sites including third party vendor sites. The Library is not responsible for the privacy practices of other sites which may be different from the privacy practices described in this policy. The Library encourages Library users to become familiar with privacy policies of other sites visited, including linked sites.

The Library website does not collect personally identifying information from visitors to the website unless the patron requests a service via the Library website. The Library may collect non-personal information from visitors to the website for statistical analysis, site assessment, server performance, authentication, troubleshooting and other management purposes. Examples of non-personal information collected include Internet Protocol (IP) address of the computer, the type and version of browser and operating system the computer uses, geographical location of the network used to link to the Library's site, and time and date of the access. There is no link to personally identifiable information in computer communications, unless a patron has provided that information in the content of a transaction, for example, filling out an online form to request a service.

The Library uses temporary "cookies" to maintain authentication when a patron is logged in to the online catalog. A "cookie" is a small text file that is sent to a user's browser from a website. The cookie itself does not contain any personally identifiable information. Other electronic services offered by the Library through third party vendors may use "cookies" to help control browser sessions. Websites may use the record of "cookies" to see how the website is being accessed and when, but not by whom. To learn more about cookies and protecting privacy online visit **OnGuard Online**.

Library database users are asked for their Library card number to ensure that only authorized users have access. Database vendors do not have access to any user records or information.

The Library and the Library System work with a variety of partners to provide e-content (e.g. e-books, e-audios, e-music, e-videos, e-magazines) to users. Prior to checking out any of the Library's e-content users should read the privacy policy of the company that is providing the service. For example, users who check out e-books from the Wisconsin Digital Library for use on their Kindle (or via a Kindle app) will receive those e-books via Amazon. Amazon's privacy policy describes the kind of information that is collected and stored in connection with such transactions. However, all other e-book formats within the OverDrive collection do not collect this information.

## **Wireless Access**

The Library offers free wireless access (Wi-Fi) for Library patrons to use with their own personal notebooks, laptops and other mobile devices. These access points are unsecured. A patron's use of this service is governed by the Library's internet policy.

Due to the proliferation of Wi-Fi networks, Library users may also be able to access other Wi-Fi networks within the building that are not provided by the Library. Use of these non-Library wireless networks within the Library's facilities is also governed by the Library's internet policy.

As with most public wireless "hotspots," the Library's wireless connection is not secure. Any information being transmitted could potentially be intercepted by another wireless user. Cautious and informed wireless users should choose not to transmit personal information (credit card numbers, passwords and any other sensitive information) while using any wireless "hotspot." Use of the Library's wireless network is entirely at the risk of the user. The Library disclaims all liability for loss of confidential information or damages resulting from that loss

## **Other services**

Some patrons may choose to take advantage of RSS feeds from the Library's website, hold and overdue notices via e-mail or text message, and similar services that send personally identifiable information related to Library use via public communication networks. Patrons should also be aware that the Library has limited ability to protect the privacy of this information once it is outside the Library's control.

## **Radio Frequency Identification (RFID)**

The Library uses RFID technology to secure and circulate its collection.

1. The only information stored on the RFID tag is the item barcode and a security bit that indicates if the item is in or out of the Library.
2. RFID technology is not used in Library cards.

## **Library Photos**

The Library takes photos at Library programs and they may be posted to the website or used in promotions. Patrons are advised to step to the side or notify Library staff members if they do not wish to be in photographs.

## **Video Surveillance**

In order to maintain a safe and secure Library, selected public areas of the Library premises may be under continuous video surveillance and recording.

Images from the Library surveillance system may be stored digitally on hardware in the library. It is the intent of the Library to retain all recorded images for a minimum of thirty days, or until image capacity of the system is reached. Then, the oldest stored images will be automatically deleted by system software to make room for new images. Typically, images will not be routinely monitored in real-time, nor reviewed by Library staff, except when specifically authorized by the Executive Director.

While it is recognized that video surveillance will not prevent all incidents, its potential deterrent effect, and resource as a means of identifying and prosecuting offenders is considered worthwhile.

Video surveillance data are considered to be protected public Library records. State Statutes carefully define law enforcement officials' authority to view surveillance data, and the Library will cooperate with law enforcement officials as permitted by Wisconsin Statutes Chapter 43.30(5) in two specific circumstances:

1. Upon the request of a law enforcement officer who is investigating criminal conduct alleged to have occurred at a Library supported in whole or in part by public funds, the Library shall disclose to the law enforcement officer all records pertinent to the alleged criminal conduct that were produced by a surveillance device under the control of the Library.
2. If a Library requests the assistance of a law enforcement officer, and the Director of the Library determines that records produced by a surveillance device under the control of the Library may assist the law enforcement officer to render the requested assistance, the Library may disclose the records to the law enforcement.

## **Illegal activity prohibited and not protected**

Patrons may conduct only legal activity while using Library resources and services. Nothing in this policy prevents the Library from exercising its right to enforce its Code of Conduct, protect its facilities, network and equipment from harm, or prevent the use of Library facilities and equipment for illegal purposes. The Library can electronically log activity to monitor its public computers and external access to its network and reserves the right to review such logs when a violation of law or Library policy is suspected. Staff is authorized to take immediate action to protect the security of Library patrons, staff, facilities, computers and the network. This includes contacting law enforcement authorities and providing information that may identify the individual(s) suspected of a violation.

## **Enforcement and redress**

Patrons with questions, concerns, or complaints about the handling of his/her personally identifiable information or this policy may file written comments with the Executive Director. A response will be sent in a timely manner and the Library may conduct an investigation or review

of practices and procedures. The Library conducts such reviews as necessary to ensure compliance with the principles outlined in this policy.

The Executive Director is custodian of Library records and is authorized to receive or comply with public records requests or inquiries from law enforcement officers. The Executive Director may delegate this authority to designated members of the Library's leadership team. The Executive Director confers with the City Attorney before determining the proper response to any request for records. The Library will not make Library records available to any agency of state, federal, or local government unless a subpoena, warrant, court order or other investigatory document is issued by a court of competent jurisdiction, showing good cause and in proper form. All Library staff are trained to refer any law enforcement inquiries to the Executive Director.

### **Breach of Security**

Any actual or suspected security breaches involving confidential information must be reported immediately to the Head of Digital Services and Innovation and the Executive Director. Incident response procedures will be initiated to identify the suspected breach, remediate the breach, and notify appropriate parties (Prairie Lakes Library System) as well as follow the Federal Trade Commission's response to a data breach.

### **Policy Changes**

This Privacy Policy may be revised to reflect changes in the Library's policies and practices or to reflect new services and content provided by the Library. Patrons are encouraged to check this document periodically to stay informed of the Library's current privacy guidelines.

### **Footnotes**

<sup>1</sup> Qualifying third parties are:

- a collection agency
- a law enforcement agency, but only if the dollar value of the individual's delinquent account is at least \$50.

<sup>2</sup> Patron records show current checkouts. When an item is returned, it is removed from the patron's checkout list. However, patrons who sign up for the reading history service will have their checkout history saved instead of purged. The user has the option to turn off the service and delete his/her reading history at any time.

## **Appendix 1**

### **Procedures for Complying with Law Enforcement Request for Information**

The Library staff will comply with law enforcement when supplied with a legal subpoena or search warrant.

### **Staff Procedures:**

If anyone approaches staff alleging to be a law enforcement official requesting information, staff will immediately contact the Executive Director. In the Executive Director's absence, the highest ranking person on duty is responsible for working with the requestor.

The Executive Director or her/his representative will ask to see official identification and will photocopy the ID.

If the law enforcement officer does not have a court order compelling the production of records, the Director or her/his representative shall explain the state statute regarding confidentiality of Library records under ss. 43.30. Staff will not disclose any information to law enforcement personnel without a court order.

If the law enforcement official presents a subpoena, the Executive Director or her/his representative will contact the City Attorney for advice on how best to proceed. It is desirable for legal counsel to be present when the subpoena is executed. In the event that the City Attorney is not available, the Deputy City Attorney will be contacted. In the event neither can be reached, the legal counsel for the American Library Association will be contacted.

If the law enforcement official presents a search warrant, it is executable immediately. The Executive Director or her/his representative will notify the City Attorney and will attempt to have legal counsel present during the search to be sure that the search conforms to the terms of the warrant. If time does not allow for this, the search must be allowed to proceed. The Executive Director or her/his representative will cooperate with the search to ensure that only the records identified in the warrant are produced and that no other users' records are viewed or scanned. Library staff should not interfere with the search and/or seizure of Library property.

The Executive Director or her/his representative will inventory any items removed from the Library as a result of the search warrant.

The Library will keep a record of all legal requests.

The Library will keep a record of all costs incurred by any search and/or seizures, including time spent by Library staff assisting in the search or the inventorying of items.

If the court order is a search warrant issued under the Foreign Intelligence Surveillance Act (FISA) (USA Patriot Act amendment), the warrant also contains a "gag order" which means that no person or institution served with the warrant can disclose that the warrant has been served or that records have been produced pursuant to the warrant. The Library and its staff must comply with this order. No information can be disclosed to any other party except legal counsel, including the patron whose records are the subject of the search warrant. Failure to comply exposes individuals to criminal and civil penalties under the USA Patriot Act. The gag order does not change the Library's right to legal representation during the search. An attorney should be called immediately, although the FBI does not have to wait until the Library receives legal



counsel before acting on the court order. If the Library's legal counsel cannot be reached, the Library Director or her/his designee, will call the ALA Office for Intellectual Freedom (OIF) at 800-545- 2433 x4223 and state only "I need to speak with an attorney." The OIF will put the caller in touch with an attorney familiar with FISA. The staff member should not inform OIF staff of the existence of the warrant.

### **Emergency Disclosures of Communication**

If the Library staff observes what could reasonably be construed as a threat of imminent danger to life, the staff member is to immediately alert local law enforcement through the 9-1-1 emergency response system and then immediately inform the highest ranking person on duty. The highest ranking person on duty should then immediately contact the Executive Director.

Approved by: RPL Board of Trustees

Approved Date: January 19<sup>th</sup>, 2023

Review Schedule: Annual.

Next Review Date: January 2024