PAULINE HAASS PUBLIC LIBRARY

POLICY: Privacy of Library Records and Library Use
Approved by Library Board: May 15, 2024

About this Policy
Protecting library user privacy is an important principle at the Pauline Haass Public Library (PHPL). This includes keeping confidential any information that identifies individuals, or that associates individuals with their use of Library materials, equipment, programs, services, facilities, and/or staff assistance. This policy affirms PHPL's commitment to privacy, explains the information that the library collects, and alerts library users 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, email or mailing address, telephone number, or any financial information relating to a patron and his or her accounts.
- **Library System** is a legal entity established under Wis. Stat. § 43. PHPL has elected to participate in a Library System and therefore benefits from shared costs for databases, collections, and services. The Library System facilitates the purchase and maintenance of the shared catalog, patron database, and digital resources. PHPL has no control over the Library System's collection of any patron information and does not use or disclose any of that information.

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. Staff procedures are included as Appendix A.

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 be disclosed only 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[1] 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. A "qualifying third party" is a law enforcement agency (but only if the dollar value of the individual's delinquent accounts is at least $50), and/or a collection agency.

Library Records

PHPL 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[2] or on hold, as well as overdue materials and fines. When an item is returned, it is removed from the cardholder's checkout list. However, cardholders who sign up for the reading history service will have their checkout history saved instead of purged. The cardholder has the option to turn off the service and delete their reading history at any time.

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. PHPL 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.

5. Emails sent to Library staff may be subject to open records requirements.

6. PHPL 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

1. **Protecting a Patron Account**
   It is the patron's responsibility to notify the PHPL immediately if a library card is lost or stolen or if the cardholder 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

2. **Keeping Account Information Up-To-Date**
   Library users may access their personally identifiable information held by the Library and are 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. Patrons may view or update their personal information in person. They may be asked to provide some sort of verification or identification card to ensure verification of identity.

3. **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).

Wisconsin State Statute 43.30(4) allows this access for custodial parents of only those children who are under age 16.

4. **Items on hold**
   Items placed on hold for library patrons are shelved by a combination of the patron's initials for pick-up in the public areas of the Library. Patrons of any age may choose to have other people pick up their holds by providing that person with their library card. To reduce errors and ensure privacy, holds can only be checked out on the card that held the item. See the Circulation Policy for more information.

Public Computer Use and the Library's Automation Systems

PHPL 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.

1. **The Library System**
   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 Internet Protocol (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.

2. **Library Website**
   PHPL maintains a website to inform library users of events, resources, services, and collections available through the library:
   - 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 website 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.

3. **Third party vendors**
   PHPL and the Library System work with a variety of partners to provide digital content (e.g. ebooks, digital audiobooks, streaming video) to users. Prior to utilizing these services and checking out any digital content, users should read the privacy policy of the company that is providing the service.

4. **Wireless Access**
   PHPL offers free wireless access (Wi-Fi) for library patrons to use with their own personal 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.

5. **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)

PHPL uses RFID technology to secure and circulate its collection. 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. RFID technology is not used in library cards.

Library Photos and Recordings
PHPL staff may record Library programs, activities, and events for use in marketing and promotions. This may include video, audio, and/or photographic recordings. If a library user does not wish to be recorded, they are advised to notify the staff member.

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.

1. 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.
2. 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.
3. Authorized staff may review surveillance camera recordings at any time and may contact law enforcement if illegal or dangerous behavior is suspected.
4. PHPL staff may observe any meeting, program, or use of any library space at any time and reserve the right to ask patrons to leave or to contact law enforcement when a violation of law or library policy is suspected.

Enforcement and Redress
Patrons with questions, concerns, or complaints about the handling of their personally identifiable information or this policy may file written comments with the 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 Library's Notice of Availability of Public Records details how public records requests are handled.

Privacy of Library Records and Library Use Policy

APPENDIX A: Staff Procedures for Complying with Law Enforcement Requests for Information

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

Staff Procedures

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

2. The Library Director or their representative will ask to see official identification and will photocopy the ID.

3. If the agent or officer does not have a **court order** compelling the production of records, the Library Director or their representative shall explain the state statute regarding confidentiality of library records under Wis. Stat. § 43.30. Staff will not disclose any information to law enforcement personnel without a court order.

4. If the court order is in the form of a **subpoena**, the Library Director or their representative will contact the Village of Sussex Municipal 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 Municipal Attorney is not available, the law offices of the Municipal Attorney will be contacted. In the event neither can be reached, the legal counsel for the American Library Association will be contacted.

5. If the court order is in the form of a **search warrant**, it is executable immediately. The Library Director or their representative will notify the Municipal 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 Library Director or their representative will cooperate with the search to ensure that only the records identified in the warrant are produced and that no other Library users' records are viewed or scanned. Library staff should not interfere with the search and/or seizure of Library property.

6. The Library Director or their representative will inventory any items removed from the Library property as a result of the search warrant.

7. The Library will keep a record of all legal requests and requests made pursuant to Wisconsin’s open records laws.

8. 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.

9. If the court order is a search warrant issued under the **Foreign Intelligence Surveillance Act (FISA)** (USA Patriot Act amendment), the procedure for a search warrant applies. However, this type of search warrant also contains a "gag order." No person or institution served can disclose that the warrant has been served or that records have been produced. The Library and its staff must comply with this order. No information can be disclosed to any other party, including the patron whose records are the subject of the search warrant.

   The gag order does not change the Library's right to legal representation during the search. Legal counsel should be called immediately, although the FBI does not have to wait until the Library receives legal counsel before acting on the court order. Contacting an attorney is not a breach of the gag order because conversations are covered by attorney-client privilege.

   If the Library's legal counsel cannot be reached, the Library Director or, in the Director's absence, Library staff member will call the ALA Office for Intellectual Freedom (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.

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 Library Director. In such an instance, the Library reserves the right to disclose otherwise protected personally identifiable information to law enforcement as deemed reasonably necessary to prevent a threat of imminent danger from materializing.

Adopted by Library Board: March 21, 2018
Reviewed and revised: May 15, 2024