Mukwonago Community Library
Confidentiality, Privacy, and Surveillance Policy
Approved October 12, 2023 – Last Reviewed October 12, 2023

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 Mukwonago Community Library (MCL). This policy affirms the MCL'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.

I. Definition of Terms

A. "Privacy" is the right to seek information through Library resources without having the subject of interest known or examined by others.

B. "Confidentiality" exists when the Library possesses personally identifiable information and keeps that information private on the Library user's behalf.

C. "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.

D. "Library System" is a legal entity established under Wis. Stat. § 43. MCL 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. MCL has no control over the Library System's collection of any patron information and MCL does not use or disclose any of that information.

II. Legal Protections and Exceptions

Wisconsin law has strong protections in place to assist public libraries 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 an 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 A to this policy.

A. The relevant Wisconsin laws concerning the confidentiality of library records are Wis. Stat. § 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.

B. Wis. Stat. § 43.30 requires that library records may only be disclosed under the following circumstances:
   i. With the consent of the individual library user.
   ii. To a custodial parent or legal guardian of a juvenile under 16 years of age.
   iii. By court order.
   iv. 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.
   v. To persons acting within the scope of their duties in the administration of the Library or library system.
   vi. To other libraries for interlibrary loan purposes in accordance with the standards set forth in Wis. Stat. § 43.30 (2) and (3).
   vii. To a qualifying third party 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.

III. Library Records

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

A. To receive a Library card, Library users are required to provide identifying information such as name, birth date, picture ID, and physical address 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 (3) years after the individual stops using the Library card at which time the record is deleted.

B. A Library cardholder's circulation record includes current identifying information, items currently checked out or on hold, as well as overdue materials and fines. Library cardholder records show current checkouts. 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.

C. Ninety (90) days after an item is returned, the Library System removes the information regarding the last user to check it out which deletes the user from the item history log. Any given item's history log is not accessible by anyone but library staff, and the information on an item's history log is only used for internal purposes. If the item had associated fines, the fine transactions are saved.

D. MCL may also gather information necessary to provide a requested service to a Library user including but not limited to the following examples:
    i. 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
    ii. Records for interlibrary loan requests or reference services
    iii. Records needed to sign up for or participate in library classes and programs
    iv. Records for use of meeting rooms
    v. 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.

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

F. MCL treats records as confidential in accordance with Wis. Stat. § 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.

IV. Access to Accounts and Patron Responsibility

A. Protecting a Patron Account

It is the patron's responsibility to notify MCL 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:

i. Log off systems after use
ii. Don't share the library card, user IDs, or passwords
iii. 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

B. Keeping Account Information Up-To-Date

A Library user may access their 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 their personal information in person. They may be asked to provide some sort of verification or identification card to ensure verification of identity.

C. Parents and Children

For the protection of Library users, parents/legal guardians seeking records of their minor child, under age sixteen (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).

D. Items on Hold

Items placed on hold for Library users are shelved for pick-up in the public areas of the Library. Library cardholders of any age may choose to have other people pick up their holds. 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.

V. Public Computer Use and the Library's Automation System

MCL 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.

A. 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.

i. 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.
ii. This information is used for internal reporting purposes and individual users are not identified.
iii. Network traffic is monitored to identify unauthorized attempts to upload or otherwise damage the web service.
iv. 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.
v. 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.
vi. MCL 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.

B. Library Website
MCL maintains a website to inform Library users of events, resources, and collections available through the Library.
i. 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.
ii. The Library's website does not collect personally identifying information from visitors to the website unless the Library user requests a service via the Library website.
iii. 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

Library user has provided that information in the content of a transaction, for example, filling out an online form to request a service.

iv. MCL's website uses temporary "cookies" to maintain authentication when a user 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.

C. Wireless Access

MCL offers free wireless access (Wi-Fi) for Library users to use with their own personal notebooks, laptops, and other mobile devices. A Library user's use of this service is governed by the Library's "Public Computers and Internet Access Policy."

i. 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 WiFi networks within the Library's facilities is also governed by the Library's "Public Computers and Internet Access Policy."

ii. As with most public WiFi "hotspots," the Library's WiFi connection is not secure. Any information being transmitted could potentially be intercepted by another WiFi user. Cautious and informed WiFi users should choose not to transmit personal information (credit card numbers, passwords and any other sensitive information) while using any WiFi "hotspot."

iii. Use of MCL's WiFi 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.

D. Other Services

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

VI. Radio Frequency Identification (RFID)

MCL 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.

VII. Library Photographs and Recordings

MCL reserves the right to utilize recordings to promote the services and programs it provides.

A. MCL does not share Library users' personally identifiable information with third parties or vendors that provide resources or Library services, unless the Library obtains explicit permission from the user or if required by law or existing contract.

B. MCL staff may record Library programs, activities, and events for use in marketing and promotions. This may include video, audio, and/or photographic recordings.
    i. The Library will post signage to indicate when recording may occur.
    ii. If a library user does not wish to be recorded, they may tell the staff member.

VIII. Video Surveillance

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

A. MCL does not use surveillance cameras to monitor, track, or profile library user's use of library resources beyond operational needs related to safety and security.

B. All footage recorded by MCL surveillance cameras is considered a "record" under Wis. Stat. § 19.32(2) and is subject to Wisconsin's Public Records Law in Chapter 19 of the Wisconsin Statutes.

C. Images from the Library surveillance system may be stored digitally on hardware in the Library. Footage is retained according to the applicable Records Disposition Authorizations approved by the Wisconsin Public Records Board, FAC00082 and FAC00082A It is the intent of the Library to retain all recorded images for a minimum of thirty (30) 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 Library Director.

D. 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.

E. Video surveillance data that indicates the identity of any individual who borrows or uses the library's documents or other materials, resources, or services 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 Wis. Stat. § 43.30 (5) in two specific circumstances:

i. 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.
ii. 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.

See Appendix B for "Surveillance Camera Usage Procedures."

IX. Illegal Activity Prohibited and Not Protected

Library users may conduct only legal activity while using Library facilities, resources, and services. Nothing in this policy prevents MCL from exercising its right to enforce its Code of Conduct; protect its facilities, network, and/or equipment from harm; or prevent the use of Library facilities and equipment for illegal purposes.

A. MCL staff is authorized to take immediate action to protect the security of Library users, staff, facilities, computers, and networks. This includes contacting law enforcement authorities and providing information that may identify the individual(s) suspected of a violation.

B. 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.

C. Authorized staff may review surveillance camera recordings at any time and may contact law enforcement if illegal or dangerous behavior is suspected.

D. MCL staff may observe any meeting, program, or use of any Library space at any time and reserve the right to ask Library users to leave or to contact law enforcement when a violation of law or Library policy is suspected.

X. Enforcement and Redress

Library users with questions, concerns, or complaints about the handling of their personally identifiable information or this policy may file written comments with the Library Director.

A. The Library Director is custodian of Library records and is authorized to receive or comply with public records requests or inquiries from law enforcement officers. The

Library Director may delegate this authority to designated members of the Library's management team.

B. A response will be sent in a timely manner and MCL 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.

C. The Library Director may confer with the Village Clerk or Municipal Attorney before determining the proper response to any request for records.

D. 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.

E. All MCL staff are trained to refer any law enforcement inquiries to the Library Director.

Revision History

October 20, 2016	Created as new standalone policy from MCL Circulation Policy with policy framework, language and research provided by the Bridges Library System
December 21, 2017	Reviewed and approved with no changes
January 17, 2019	Changed language under 'Items to Hold' in Section 'Access to Accounts and Patron Responsibility' to "Items placed on hold for library patrons are shelved for pick-up in the public areas of the Library."
January 17, 2019	Changed language under Section 'Illegal activity prohibited and not protected' from "exercising its right to enforce its Rules of Behavior" to "exercising its right to enforce its Code of Conduct".
October 12, 2023	Inserted "Surveillance Camera Usage Procedures" and renamed policy from "Confidentiality and Privacy Policy" to "Confidentiality, Privacy, and Surveillance Policy" Policy updated for clarity and consistency throughout Updated references to other policies throughout Reviewed by Village legal counsel

Appendix A

Mukwonago Community Library
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 MCL 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.
- The Library Director or their 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 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.
- If the law enforcement official presents a subpoena, the Library Director or their representative will contact the 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.
- If the law enforcement official presents 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.
- The Library Director or their representative will inventory any items removed from the Library property as a result of the search warrant.
- The Library will keep a record of all legal requests and requests made pursuant to Wisconsin’s open records laws.
- 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 Library user 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 their 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 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.

Appendix B

Mukwonago Community Library
Surveillance Camera Usage Procedures

The Library's surveillance cameras generate a record of activities in monitored areas of the Library building and property. In the event of illegal activities in these areas, it may be necessary to review the recordings.

This procedure details who may review the records and under what circumstances they may be viewed and/or released to law enforcement personnel.

Reviewing the Surveillance Camera Recordings

- In the event of suspicious or illegal activity being reported in areas covered by the surveillance cameras, a staff member may request that the Library Director or their designee review the recordings.
- The staff member should request that the Library Director or their designee run the footage of the incident while they and the staff member are present.
- Staff are not to review a security recording without the Library Director or their designee being present.

Reviewing the Surveillance Camera Recordings With the Authorities

- In the event of suspicious or illegal activity being observed on review of the recordings, law enforcement may be contacted.
- In the event that law enforcement officers wish to review the recordings, the same procedure used for initial review of the tape will be followed with a law enforcement officer present, i.e., a staff member should request that the Library Director or their designee run the recordings of the incident while they, the staff member, and the law enforcement officer are present.

Release of the Surveillance Camera Recordings

- Upon a request by the authorities to release the recordings in order to pursue further investigations, the Library Director may release a burned CD/DVD copy or MP4 digital copy to the requesting officer. The Library Director must obtain name, signature, badge number, date and time from the requesting officer and append it to the Library incident report along with the notation "Surveillance recording released to: [name]".
- Upon a request by those other than law enforcement, please refer to section II "Legal Protections and Exceptions" of the Confidentiality, Privacy, and Surveillance Policy referring to Wis. Stat. § 43.30 and under what circumstances such Library records may be disclosed.