Trustee Workshop:

Patron Privacy and Access Policies

OWWL Library System

Agenda

I. Why We're Discussing This Now
II. Introduction to Patron Privacy in Libraries
III. Data Breaches and Cyber Attacks in Libraries
IV. System Access and Confidentiality of Library Records Policy
V. FAQ on Patron Data and Privacy
VI. Questions

Why are we Discussing Patron Privacy Now?

Why Are We Discussing This Now?

- Patron privacy has always been a concern for libraries; this is an evolution of System-wide data handling policies.
- Data breaches are happening at an alarming rate.
- Previous policies were agreed to by Directors; now it will be Member Library Boards for buy-in and support.
- All libraries should understand the limitations on use of patron data, how it is stored, how it is protected, and how to use it appropriately.

Introduction to Patron Privacy in Libraries

Responsibilities of Libraries

- The library profession has a long-standing ethic of facilitating, not monitoring, access to information.
- It is essential that libraries maintain an updated policy on data practices.
- Everyone who provides governance, administration, or service in libraries, including volunteers, has a responsibility to maintain an environment respectful and protective of the privacy of all users.
- Libraries should not monitor, track, or profile an individual's library use beyond circulation needs.
- Data collected for analytical use should be limited to anonymous or aggregated data and not tied to individuals' personal data.

Civil Practice Law Section 4509, Library Records

§ 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.*

Source: https://www.nysenate.gov/legislation/laws/CVP/4509

Civil Practice Law Section 4509, Library Records

1. All patron activity in a library and records from library use is confidential and protected by law.
2. Libraries are responsible for ensuring that patron personally identifiable information *and* library usage are not shared with any person or business outside of the agreements between the library and the patron.

Office of the State Comptroller

1. Increased number of audits focusing on:
    - Cybersecurity;
    - Account Management;
    - Passwords; and
    - Data Retrieval

New York Privacy Act

1. Draft legislation looking at:
    - Consumer Privacy Protection;
    - Consumer Rights;
    - Sharing, processing, and sale of data;
    - Responsibilities/obligations for those who control/process the data; and
    - How organizations handle and safeguard consumers data.

What is OWWL Library System Doing to Protect Patron Data?

1. Limit third-party vendor access to patron data.
2. Negotiate contracts to ensure patron privacy.
3. Carry cyber liability coverage in the event of a System-wide data breach involving member libraries.
4. Ongoing policy development in the areas of data breaches, privacy policies, email usage, and situations involving patron information.
5. Forming a Data Security Program to…
    - Identify internal and external risks;
    - Assesses the sufficiency of safeguards;
    - Train staff;
    - Select service providers; and
    - Adjust security programs as needed.

Current Concerns of Patron Data and Libraries

Current Concerns of Patron Data and Libraries

1. Using patron data beyond circulation needs.
2. Password security for ILS and email accounts containing patron data.
3. Cyber attacks and phishing scams.
4. Insecure transmission of patron data locally.
5. Allowing unauthorized third-party access of patron data.
6. Limiting the amount of Personally Identifiable Information contained in the ILS.
7. Lack of “opt-in” procedures for patron communication outside circulation needs.

Patron Opt-In vs. Opt-Out

- Use of patron data beyond what is required for circulation should ***not*** be an "opt-out" option by default.
    - "users should have the choice to opt-in to any data collection that is not essential to library operations and the opportunity to "opt-out" again at any future time."
    - All nonessential data collection should be turned off by default.
- "In all areas of librarianship, best practice leaves users in control of as many choices as possible regarding their privacy. This includes decisions about the selection of, access to, and use of information. Information about options available to users should be prominently displayed, accessible, and understandable for a general audience."
    - Source: ALA, Privacy: An Interpretation of the Library Bill of Rights.

Patron Opt-In vs. Opt-Out

- The American Library Association goes on to say that users should have the right to give "explicit consent."
  - "Explicit consent means that users are given an option to agree or disagree with the collection of their data. The user must be informed in a specific and unambiguous manner regarding how their data will be collected, used, and/or shared. Users should be given the choice before choosing to access a service rather than have to opt-out later. Libraries should ensure their online services do not default to opt-out. Opt-out requires action from the user to remove themselves from data collection. This does not allow a user to learn about the specific details of how their data will be utilized."
    - Source: Privacy and Confidentiality Q&A
- OWWL Library System does not have the capabilities nor the infrastructure to track opt-in consent in the ILS; libraries should follow local procedures when performing this task.

Patron Opt-In vs. Opt-Out

- While libraries are barred from using patron data for mailing lists or other communications outside of overdue notices, a library can certainly create an "opt-in" option on their library registration card or renewal procedure to include patrons on a mailing list or other service.
    - Adding a line such as "Per our patron confidentiality policy, the library considers records of your patronage confidential. Do you consent to the library using your name and address for newsletter information, event notification, and fund-raising? If so, please sign the agreement below. We won't supply your information to any third party, and our mailings will come straight from the library!”

Data Breaches and Cyber Attacks - Examples in Libraries

1. **Buffalo & Erie County Public Library System** (Ransomware attack on Internal Database) - 2020
2. **Boston Public Library** (Cyber Attack Took System Offline) - 2021
3. **OWWL Library System Member Library** (Compromised Email) - 2021
4. **Westchester Library System** (Ransomware Attack) - 2022
5. **Rochester, MN** (~1,700 Patron Records) - 2022
6. **Whatcom County Library System** (735 Patron Records) - 2022
7. **OWWL Library System Member Library** (Compromised Email) - 2022

Data Breaches and Cyber Attacks - Examples in Libraries

1. **Buffalo & Erie County Public Library System** (Ransomware attack on Internal Database) - 2020
2. **Boston Public Library** (Cyber Attack Took System Offline) - 2021
3. **OWWL Library System Member Library** (Compromised Email) - 2021
4. **Westchester Library System** (Ransomware Attack) - 2022
5. **Rochester, MN** (~1,700 Patron Records) - 2022
6. **Whatcom County Library System** (735 Patron Records) - 2022
7. **OWWL Library System Member Library** (Compromised Email) - 2022
    a. Secured account;
    b. Evaluated scale of attack/breach;
    c. Notified patrons;
    d. Notified District Attorney;
    e. Worked with legal team;
    f. Ended up being a costly endeavor.

Systems Access and Confidentiality of Library Records Policy

History

1. Originally drafted as a procedure governing Library use of patron data in February 2021.
2. Presented to Directors as a Draft System Policy in April 2021.
3. Reviewed by the Evergreen Advisory Committee in May 2021
4. Approved by Directors Advisory Council in September 2021.
5. Formally approved as a policy in September 2021.
6. Notice of Directors to Sign Agreement form April 2022.
7. Agreed to by all 42 Library Directors by July 2022.
8. Reviewed by System Attorney for accuracy and clarification June 2022.
9. System Board add additional definitions and clarifying language in June 2022.
10. Reviewed by separate committee of Trustees and Library Directors March 3, 2023
11. ALA Committee on Intellectual Freedom wrote a letter supporting the policy in March 2023.
12. Policy Committee and System Board reaffirmed the policy in March 2023.
13. System Board updates policy for Member Library Board Agreement in April 2023.
14. System Board updates Member Library Board Agreement based on Member Library feedback in June 2023.

What is the Systems Access Policy?

The Systems Access and Confidentiality of Library Records Policy aims to establish practices for maintaining the information security of the Personally Identifiable Information (PII) collected and stored by libraries and the OWWL Library System. This policy shall apply to all individuals authorized to access the System Information Systems as necessary for their job functions.

What is the Systems Access Policy?

Set of rules and guidelines to protect patron information.

What does the policy cover?

1. Managing user accounts with access to patron data.
2. Stipulating password requirements for data protection.
3. Electronic Security and Physical Security.
4. Managing Files Containing Patron PII.
5. Appropriate Use and Collection of Patron Data.
6. Requests for Information from Law Enforcement Agencies.
7. Member Library Agreement.
8. System Staff Agreement.
9. Policy Justification and Resources.

Managing User Accounts

1. When someone joins or leaves your library staff, account actions need to take place as soon as possible.
    a. This is to protect against unauthorized access to the patron database.
2. Shared accounts must be kept to a minimum and avoided whenever possible. When not avoidable, passwords must be changed upon separation of one or more employees with access to the shared account.

Passwords

1. National Institute of Standards and Technology (NIST) Guidelines
    a. Passwords used to access the System Information Systems that contain patron PII shall be:
        i. Randomly generated;
        ii. At least 12 characters long;
        iii. Unique; and
        iv. Should contain some level of complexity.
    b. Passwords shall not:
        i. Consist of previously used passwords;
        ii. Consist of passwords used for personal accounts;
        iii. Be shared with others; or
        iv. Stored on shared computers.

Electronic Security and Physical Security

1. Electronic Security
    a. Device must be library-owned;
    b. Device must be designated only for staff use (i.e., should not be lent to the public);
    c. Device must have an up-to-date operating system;
    d. Device must have up-to-date virus protection;
    e. Device must have an up-to-date web browser; and
    f. No files containing Patron PII shall be downloaded or stored on personal computers.
2. Physical Security
    a. 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.
    b. Devices on which patron PII is stored or accessed should be properly secured against unauthorized access. Only library staff members should be authorized to access devices used to log on to System Information Systems (i.e., Evergreen and Email services).

Managing Files Containing Patron PII

1. Best Practices:
    a. Accessing files or any links to files only on library-owned equipment and avoiding using personally-owned computers, mobile devices, and services, like Dropbox, to access, save, or store files.
    b. Making sure that files and printed copies are kept secure from unauthorized access.
    c. Avoiding transmitting files using methods that may not be secure, such as by email attachment. Instead, transmit files by using a shared drive on your local network or removable media like a flash drive.
    d. Avoiding sharing files with, or uploading files to, unauthorized third-parties or third-party services.
    e. Deleting files and emptying the recycling bin/trash when you are done with them.
    f. Shredding any printed copies when you are done with them.

Appropriate Use of Patron Data

1. 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. Libraries may also directly communicate with a patron about issues with their account. No other access is assumed or approved when accessing PII.
2. Patron PII should never be exported from any of the System 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, newsletter platforms, Dropbox, and Google Drive.

Requests for Information from Law Enforcement Agencies

1. Law enforcement agencies are required to have a subpoena in order to access any patron information from the library.

Member Library Agreement

1. Staff must use their authorized access to Information Systems only to complete their work responsibilities in full compliance with this policy.
2. Staff must comply with all controls established by the OWWL Library System regarding the use of Information maintained within the defined Information Systems.
3. Staff are prohibited from the disclosure of Information including any PII, circulation information, or information about a patron's usage of the library, contained in Information Systems to unauthorized persons and third parties without the explicit consent of the OWWL Library System except as permitted under applicable OWWL Library System policy and Federal or State law.
4. Staff must exercise care to protect Information against accidental or unauthorized access, modifications, disclosures, or destruction.
5. Staff understands that the obligation to avoid such disclosure will continue even after they leave the employment of a Member Library.
6. The Member Library understands that any violation of this Agreement or other System policies related to the appropriate release of or disclosure of Information may result in one or more sanctions, including termination of library access to Information Systems, termination of System support services, criminal penalties, or civil liability.

What is My Library Agreeing To?

1. To protect patron data in a responsible way.
    a. Staff can only use Evergreen for their job (i.e. checking in and checking out library materials).
    b. Staff must keep patron information private.
        i. This includes acting responsibly with access, passwords, and usage of data.
    c. Staff cannot provide patron information to anyone who is not authorized to access information.
    d. The library must adhere to all State Laws regarding privacy.

Who Else Agrees to This?

1. All System Staff agree to these terms.
2. We review all contracts negotiated with third-parties (i.e., OverDrive, Ancestry, Mango Languages, etc.) to be assured of data practices.
    a. Data is limited with third-part vendors through contracts or through System practices.

How Does a Member Library Agree to this Policy?

1. Approve locally however you typically approve agreements.
2. Send Ron a copy of the form and the minutes where your board approved.
3. This will happen annually.

Member Library Agreement Form

As a Member Library of the OWWL Library System, _____ Library understands that only authorized library employees shall have access to data, information, and records (all hereinafter referred to as Information) maintained in OWWL Library System's Information Systems (as defined above in the "Definitions" section of this policy). Such employee access is limited to what is needed to effectively deliver library services.

The OWWL Library System requests that Member Library Boards formally vote and adopt a Board Motion following local agreement practices, or alternatively create a local policy, and/or enact a similar action agreeing to the following:

Our library affirms that _____ Library has been advised of, understands, and agrees to the following terms and conditions for library employee access to Information Systems managed by OWWL Library System.

1) Staff must use their authorized access to Information Systems only to complete their work responsibilities in full compliance with this policy.
2) Staff must comply with all controls established by the OWWL Library System regarding the use of Information maintained within the defined Information Systems.
3) Staff are prohibited from the disclosure of Information including any PII, circulation information, or information about a patron's usage of the library, contained in Information Systems to unauthorized persons and third parties without the explicit consent of the OWWL Library System except as permitted under applicable OWWL Library System policy and Federal or State law.
4) Staff must exercise care to protect Information against accidental or unauthorized access, modifications, disclosures, or destruction.
5) Staff understands that the obligation to avoid such disclosure will continue even after they leave the employment of a Member Library.
6) The Member Library understands that any violation of this Agreement or other System policies related to the appropriate release of or disclosure of Information may result in one or more sanctions, including termination of library access to Information Systems, termination of System support services, criminal penalties, or civil liability.

***Sample Board Motion**: _____ Library affirms the governance responsibilities of the Board of Trustees, including the oversight and support of the Library Director in the management actions required to comply with all provisions of the Systems Access and Confidentiality of Library Records Policy, relevant OWWL Library System policies, respective local policies, and other NYS Laws referenced therein, to protect patron privacy and the patron data entrusted to _____ Library and OWWL Library System.*

Member Library Representative Name Signature Date

Please include a copy of the Meeting Minutes when the motion was approved.

Frequently Asked Questions on Patron Data and Privacy

How do we get staff to change password habits?

- ➔ Emphasize the importance of security and help them understand the root causes of data breaches.
- ➔ Educating employees about password best practices.
- ➔ Discuss using password managers.

What patron reports can OWWL Library System provide?

- ➔ Your request may be most appropriately fulfilled by aggregated data.
- ➔ If you are looking for more information on how many items patrons are checking out in the past year, you may wish to request a breakdown of the counts rather than a list of specific patrons and their number of checkouts.
- ➔ If you are performing maintenance on patron records in Evergreen, you may need to request a list of your patrons based on specific attributes.
  - ◆ For example, you may have changed the age at which your library considers a patron a juvenile and wish to update patron records based on their date of birth (though we are happy to help you automate this change).

Who else is talking about data privacy?

- ➔ The New York Privacy Act (A7423).
  - ◆ This is an expansive consumer privacy protection act that delineates consumer rights around the sharing, processing, and sale of their data, as well as the responsibilities/obligations that those who control/process the data have around how they handle and safeguard consumers data.
- ➔ Office of the State Comptroller
  - ◆ Towns, Villages, and School District have been cited in many recent OSC audits for having inappropriate user account practices.
  - ◆ “Cybercrimes continue to rise. According to the Federal Bureau of Investigation (FBI), complaints of phishing and similar cyberattacks often used to deliver ransomware increased by 162%, from 114,702 in 2019 to 300,497 in 2022. These attacks can have a significant impact on the public when they target public authorities and local governments that oversee a variety of services the public depends on, including water systems, utilities, airports, schools, and health care facilities. In 2022, there were 2,385 complaints of ransomware, according to the FBI’s Internet Crime Report.” OSC Audit - Cyber Incident Response Team (Follow-Up)
- ➔ Broader conversation at Library Systems in New York.

Questions?