Systems Access and Confidentiality of Library Records Policy

Summary

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.

This policy outlines practices for the following:

1) Creation and deletion of staff user accounts;
2) Generating secure passwords;
3) Electronic and physical access of library systems and devices; and
4) Appropriate dissemination of the PII contained in library systems.

Purpose

Protecting patron privacy and confidentiality is a core principle of librarianship. The American Library Association's Library Bill of Rights, Article VII, states that:

> *[a]ll people, regardless of origin, age, background, or views, possess a right to privacy and confidentiality in their library use. Libraries should advocate for, educate about, and protect people's privacy, safeguarding all library use data, including personally identifiable information.*[3]

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

> *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*

[3] ALA Library Bill of Rights, http://www.ala.org/advocacy/intfreedom/librarybill

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.[4]

The OWWL Library System also acknowledges its responsibilities under New York's Stop Hacks and Improve Electronic Data Security Act ("SHIELD Act") to develop, implement, and maintain reasonable security safeguards to prevent the unauthorized release of personal information.

Definitions

Personally Identifiable Information (PII)

Patron PII is generally data about a patron. Examples include a patron's name, address, email address, telephone number, or date of birth, either alone or in combination. Additional data about patrons, data about activity that can be tied back to a patron, is also collected and stored in the System Information Systems and should also be considered confidential. Examples of these types of data include a patron's circulation history, hold requests, or paid bills. For the purposes of this policy, the term "patron PII" describes all confidential information about a patron whether or not it is traditionally considered PII.

OWWL Library System collects the minimum personally identifying information (PII) necessary to conduct library-related business, including the circulation of library materials, contacting library patrons regarding library transactions and services, and connecting to third-party services that support library services.

OWWL Library System maintains certain administrative information regarding the use of the System Information Systems and managed computer services accessed by individuals through member libraries or via remote access. This information is kept for administrative purposes only.

Integrated Library System (ILS)

The ILS supported and maintained by OWWL Library System is Evergreen.

OWWL Library System Information Systems

Information Systems maintained by OWWL Library System, including those that may contain patron PII. These include, but are not limited to email, the ILS, the System reporting tool, LibCal, and Prefab Websites.

[4] New York Civil Practice Law, Sec. 4509, Library Records, https://newyork.public.law/laws/n.y._civil_practice_law_section_4509#:~:text=Library%20records%2C%20which%20contain%20names,library%20materials%2C%20computer%20database%20searches%2C

Scope

This policy shall apply to all individuals authorized to access the System Information Systems as necessary for their job functions.

Accounts and Passwords

This portion of the policy establishes that both adequate controls on accounts and appropriate password management and construction are important aspects of maintaining the security of systems that hold patron PII and protecting patron confidentiality.

Account Creation and Removal

- System IT staff should be notified of any personnel changes at a library that would require either the issuance of credentials to access the System Information Systems (such as email or the ILS) or the termination of access to the System Information Systems.
- Notifications of separations of service to the System should occur immediately to ensure that individuals who should no longer have access to the System Information Systems are removed as authorized users. Whenever possible, notification of separation of service should occur in advance of the date of separation.
- Library directors or their designees are responsible for informing OWWL Library System of the separation from service of an individual who has/had access to a shared account (detailed below).
- A library's board president is responsible for informing OWWL Library System of the separation from service of a library director.

Shared Accounts

- Shared accounts should be kept to a minimum and avoided whenever possible. When not able to be avoided, passwords shared between multiple authorized individuals shall be changed upon the separation from service of an individual no longer authorized to access the System Information Systems. The responsibility to ensure that passwords are changed ultimately rests with the library director.
- Shared accounts include accounts that may be accessed by only one authorized individual at a time but which shall continue to be used after an individual's separation from service.
    - Any such accounts should also have their passwords changed upon a handover.
- Examples of appropriate shared accounts include:
    - A library's circulation email account.
    - An ad hoc email account created for a search committee.

Passwords

- Passwords used to access the System Information Systems that contain patron PII shall be:

    - Randomly generated[5];
    - At least 12 characters long;
    - Unique; and
    - Should contain some level of complexity.
- Examples of adequate passwords include:
    - A "diceware" password[6] (a string of randomly generated dictionary words)
        - If using a "diceware" password, the password shall consist of a minimum of five randomly generated words.
    - A password that is at least 12 random characters long.
- Passwords shall not:
    - Consist of previously used passwords; or
    - Consist of passwords used for personal accounts.
- Passwords used to access the System Information Systems shall not be transmitted in plain text (such as by email).
    - An exception can be made for passwords transmitted for one-time use, i.e. passwords used for an initial login that the recipient should then change after they are able to access the system.
- If an account or password is suspected to have been compromised, report the incident to System staff immediately by emailing support@pls-net.org.

Accessing the System Information Systems

This portion of the policy establishes that both the electronic and physical security of devices used to access the System Information Systems is important for maintaining the security of the network as a whole.

Electronic Security

- Only devices meeting all of the following requirements shall be used to access the ILS or the System reporting tool with staff credentials:
    - Device must be library-owned;
    - Device must be designated only for staff use (i.e., should not be lent to the public);
    - Device must have an up-to-date operating system;
    - Device must have up-to-date virus protection; and
    - Device must have an up-to-date web browser.
- No file containing patron PII should be downloaded to or stored on personal devices.
    - Such files include, but are not limited to:
        - files generated by the ILS;
        - files transmitted via email; or

[5] Use a password generator to create a password. Password generators are often offered by password managers, like the generators offered by 1Password (https://1password.com/password-generator/) or LastPass (https://www.lastpass.com/password-generator).
[6] The EFF (Electronic Frontier Foundation) offers a guide to, and tool for, generating passwords by dice: https://www.eff.org/dice

        - files accessed on the System reporting tool.

Physical Security

- Devices on which patron PII is stored or accessed should be properly secured against unauthorized access.
- 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.

Management of Files, Reports, and/or Documents Containing Patron PII

Best practices for handling files, reports, and/or documents containing patron PII include, but are not limited to:

- 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.
- Making sure that files and printed copies are kept secure from unauthorized access.
- 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.
- Avoiding sharing files with, or uploading files to, unauthorized third-parties or third-party services.
- Deleting files and emptying the recycling bin/trash when you are done with them.
- Shredding any printed copies when you are done with them.

Storing and Accessing PII

This portion of the policy establishes what types of data about patrons should be stored in the System Information Systems and how patron PII accessed in the System Information Systems may be used.

Data collected about library patrons and transactions is used only to conduct library-related business, the administration of library services, and to assist the specific person to whom the information pertains.

Appropriate Collection of Data

- Only data necessary to provide library services should be stored in shared the System Information Systems (like the ILS). The least amount of personally identifiable information possible should be collected and stored in the System Information Systems.
    - Examples of data appropriate for collection include, but are not limited to:
        - Name
        - Address
        - Email address
        - Telephone number

        - Date of birth
    - Examples of data inappropriate for collection include, but are not limited to:
        - Health information
        - Driver's license numbers
- Data about patrons should only be stored in the System Information Systems for the length of time necessary for operational or legal purposes.

Appropriate Use of Data

- Patron PII should be used only for providing library services, such as for contacting patrons to inform them of available holds, overdue materials, etc.
- Any use of patron PII accessed from the System Information Systems beyond providing library services must be a use to which a patron has explicitly consented to and opted-in.
- Patron PII should never be exported from any the System Information Systems for the purpose of being shared with or uploaded to any third-party or third-party services.
    - Examples of third-parties include, but are not limited to, Friends groups and foundations.
    - Examples of third-party services include, but are not limited to, fundraising platforms, Dropbox, and Google Drive.

Requests for Information from Law Enforcement Agencies

No Member Library staff or System staff other than the director or director's designee is authorized to respond to any form of judicial process or to provide any patron-specific or library-business information, in writing or in oral form, to a law enforcement officer or other person.

No individual data or transactions may be divulged to third parties except by court order.

In the event a the System Member Library staff person or System staff person is requested to provide patron information to any outside agency or individual the following procedures or appropriate local library procedures must be followed:

1) The staff member receiving the request to examine or obtain information relating to circulation, computer activity or other records identifying the names of library users, will immediately ask for identification, then refer the person making the request to the director, or designee in the director's absence, who shall explain the institution's confidentiality policy. The staff member will not disclose any information.
2) The director, upon receipt of a process, order, or subpoena, shall consult with legal counsel to determine if such process, order, or subpoena is in good form and if there is a showing of good cause for its issuance. The Director should contact the System Executive Director.
3) If the process, order, or subpoena is not in proper form or if good cause has not been shown, insistence shall be made that such defects be corrected before any records are released. Without documents in proper form, law enforcement has no authority to compel disclosure of any information, other than the name of the person speaking to law enforcement officers.

4) Any threats or unauthorized demands (i.e., those not supported by a process, order, or subpoena) concerning circulation, computer or other records identifying the names of library users shall be reported to the director immediately.
5) If the document is a search warrant that authorizes immediate search and seizure, inform the officer that the library director and legal counsel will be contacted immediately and request the patience of the officer. (The officer may inform you that the warrant is "secret". This does not preclude notification of the director and legal counsel.) If the officer declines to wait, carefully inspect the warrant and monitor the search.
6) Retain a copy of the warrant and request an inventory of the materials in question. Offer the officer a copy of any data requested. At the conclusion of the search immediately make a written record of all events that transpired.
7) Add the copy of the warrant, request documents, and the written record of the event to your incidents file or appropriate storage area.

Employee Confidentiality Agreement

All the System Member Library and System staff, in order to have access to the System Information Systems, are required to read this policy and agree to its contents. Agreement indicates their understanding that access to these systems, manual and automated, containing PII and other library record data is limited to the requirements of their job, and such information is not to be disclosed to unauthorized persons.

Member Libraries may collect agreements from staff using any form they wish providing the agreement upholds this policy. Member Libraries will be required to attest to the System on an annual basis that all staff have agreed to the provisions in this policy. As new or promoted staff are expected to perform tasks involving patron information, the policy must be presented and agreed to by said staff member(s).

Amended: June 8, 2022
Adopted: September 8, 2021