OWWL Library System

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.[1]

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.

---

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

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.[2]

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.

Third Party Services

---

[2] 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

A third party is considered any person, group, vendor, or company other than the OWWL Library System and member libraries.

Third party access to patron data is prohibited except when authorized explicitly, in writing or contract, by the OWWL Library System.

In instances of third party access, the OWWL Library System will make every effort possible to limit the amount of patron PII accessible by the third party to only what is needed to provide the service.

An example of current third party services with limited patron PII access is OverDrive for the Systems eBook and Audiobook collection.

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 (Evergreen), the System reporting tool, LibCal, and Prefab Websites.

Patron Consent

When completing a library card application at a member library, the patron consents for their data to be used for 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 registering for a library card.

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.
  o Any such accounts should also have their passwords changed upon a handover.
- Examples of appropriate shared accounts include:
  o A library's circulation email account.
  o 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:
  o Randomly generated[3];
  o At least 12 characters long;
  o Unique; and
  o Should contain some level of complexity.
- Examples of adequate passwords include:
  o A "diceware" password[4] (a string of randomly generated dictionary words)
    ▪ If using a "diceware" password, the password shall consist of a minimum of five randomly generated words.
  o A password that is at least 12 random characters long.
- Passwords shall not:

---

[3] 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).
[4] The EFF (Electronic Frontier Foundation) offers a guide to, and tool for, generating passwords by dice: https://www.eff.org/dice

- o Consist of previously used passwords; or
- o 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).
  - o 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@owwl.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 purchased through OWWL Library System's mediated PC purchasing program and configured by OWWL Library System may be used to access Information Systems (including the ILS and System Reporting tool) with staff credentials. The System will ensure devices meet the following requirements:
  - o Device must have an up-to-date operating system;
  - o Device must have up-to-date virus protection; and
  - o Device must have an up-to-date web browser.
- Member Libraries will ensure devices meet the following criteria:
  - o Devices are library-owned, purchased, and configured through OWWL Library System;
  - o Devices must be designated only for staff use (i.e., should not be lent to the public); and
  - o Devices may only be accessed by staff accounts that adhere to this policy.
- No file containing patron PII should be downloaded to or stored on personal devices.
  - o Such files include, but are not limited to:
    - ▪ files generated by the ILS;
    - ▪ files transmitted via email; or
    - ▪ files accessed on the System reporting tool.
- When using shared computers or browsers, staff should avoid saving login credentials (usernames and passwords) used to access System Information Systems to a browser's password manager. Dedicated password managers which can be logged into and out of are a secure way of managing multiple passwords on shared computers and browsers.

Physical Security

- 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.

- 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).

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

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.

<u>Appropriate Collection of Data</u>

- 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.

<u>Appropriate Use of Data</u>

- 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.
- Local patron opt-in does not authorize the library to use data from Evergreen or any other System-provided information systems.
- 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.
    - 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.
    - 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 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.

Member Libraries and System Access

In order for Member Libraries to maintain access to Information Systems managed by OWWL Library System (including, but not limited to, email, the ILS (Evergreen), the System reporting tool, LibCal, and Prefab Websites), Member Libraries must follow all aspects of this policy.

By participating in the use of OWWL Library System's Information Systems, all libraries agree to the following standards:

1. 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.
2. Staff must use their authorized access to Information Systems only to complete their work responsibilities in full compliance with this policy.
3. Staff must comply with all controls established by the OWWL Library System regarding the use of Information maintained within the defined Information Systems.
4. 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.
5. Staff must exercise care to protect Information against accidental or unauthorized access, modifications, disclosures, or destruction.
6. Staff understand that the obligation to avoid such disclosure will continue even after they leave the employment of a Member Library.
7. 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.

Member Library Directors should regularly ensure staff members and Trustees understand that access to Personally Identifiable Information (PII) and other library record data contained in OWWL Library System's Information Systems is limited to the requirements of library work and patron consent (as defined above in the "Definitions" section of this policy), and such information is not to be disclosed to unauthorized persons and must be kept secure at all times.

Member Libraries will be held responsible and liable for any local infraction of this policy. Member Libraries may wish to collect local agreements from staff using any form they deem appropriate, providing the agreement upholds this policy. Libraries are welcome to use this policy's System Staff Agreement Form below as a sample form.

System Staff Acknowledgment Form

I understand that my access to data, information, and records (all hereinafter referred to as Information) maintained in the manual and automated information and records systems (all hereinafter referred to as the System Information Systems) of the OWWL Library System is limited by my needs for the information in the performance of my job duties.

By my signature below, I affirm that I have been advised of, understand, and acknowledge the following terms and conditions of my access to Information contained in the System Information Systems.

1) I will use my authorized access to Information Systems only in the performance of the responsibilities of my position as an employee of a member library or direct employee of the System.
2) I will comply with all controls established by the System regarding the use of information maintained within the System Information Systems.
3) I will avoid disclosure of Information to unauthorized persons without the appropriate consent of the Information owner except as permitted under applicable the System policy and Federal or State law. I understand and agree that my obligation to avoid such disclosure will continue even after I leave the employment of a member library or the System.
4) I will exercise care to protect Information against accidental or unauthorized access, modifications, disclosures, or destruction.
5) When discussing Information with other employees in the course of my work, I will exercise care to keep the conversation private and not overheard by others who are not authorized to have access to such information.
6) I understand that any violation of System policies related to the appropriate release of or disclosure of Information may result in one or more sanctions, including immediate termination of my access to the System Information Systems, criminal penalties, or civil liability.

I affirm that I have been given the opportunity to review the Systems and Confidentiality of Library Records Policy and other NYS and the System policies referenced therein, and I further affirm that my questions about those policies have been answered to my satisfaction.

_____   _____
Employee Name   Title

_____   _____
Employee Signature   Date

Policy Justification Resources

NIST (National Institute of Standard and Technology): Digital Identity Guidelines: Authentication and Lifecycle Management (SP 800-63B)[5]

Q-B05: Is password expiration no longer recommended? [6]

> *A-B05:*
>
> *SP 800-63B Section 5.1.1.2 paragraph 9 states:*
>
> *"Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically). However, verifiers SHALL force a change if there is evidence of compromise of the authenticator."*
>
> *Users tend to choose weaker memorized secrets when they know that they will have to change them in the near future. When those changes do occur, they often select a secret that is similar to their old memorized secret by applying a set of common transformations such as increasing a number in the password. This practice provides a false sense of security if any of the previous secrets has been compromised since attackers can apply these same common transformations. But if there is evidence that the memorized secret has been compromised, such as by a breach of the verifier's hashed password database or observed fraudulent activity, subscribers should be required to change their memorized secrets. However, this event-based change should occur rarely, so that they are less motivated to choose a weak secret with the knowledge that it will only be used for a limited period of time.*

Q-B06: Are password composition rules no longer recommended?[7]

> *A-B06:*
>
> *SP 800-63B Section 5.1.1.2 paragraph 9 recommends against the use of composition rules (e.g., requiring lower-case, upper-case, digits, and/or special characters) for memorized secrets. These rules provide less benefit than might be expected because users tend to use predictable methods for satisfying these requirements when imposed (e.g., appending a ! to a memorized secret when required to use a special character). The frustration they often face may also cause them to focus on minimally satisfying the requirements rather than devising a memorable but complex secret. Instead, a blacklist of common passwords*

---

[5] Digital Identity Guidelines, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf
[6] NIST Special Publication 800-63: FAQ, Q-B05, https://pages.nist.gov/800-63-FAQ/#q-b05
[7] NIST Special Publication 800-63: FAQ, Q-B06, https://pages.nist.gov/800-63-FAQ/#q-b06

prevents subscribers from choosing very common values that would be particularly vulnerable, especially to an online attack.

Composition rules also inadvertently encourage people to use the same password across multiple systems since they often result in passwords that are difficult for people to memorize.

Q-B10: Does SP 800-63B require that we remove our password composition (complexity) rules?[8]

> *A-B10:*

> *SP 800-63B Section 5.1.1.2 states in part:*

> *Verifiers SHOULD NOT impose other composition rules (e.g., requiring mixtures of different character types or prohibiting consecutively repeated characters) for memorized secrets.*

> *This text is a recommendation, not a normative requirement (i.e., "should" rather than "shall" in text). However, research has shown that composition rules do not significantly improve the security of selected passwords. Composition rules often have the opposite effect as users tend to avoid or shortcut the rules by making predictable changes, resulting in weaker passwords and less security. Instead, SP 800-63B requires the use of a blacklist of common passwords that are not acceptable for use. We do recommend increased password length as a key password security control, especially through encouraging the use of passphrases.*

NIST (National Institute of Standard and Technology): Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (SP 800-122)[9]

> *2.3 PII and Fair Information Practices*

> *Purpose Specification—The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.*

> *Use Limitation—Personal data should not be disclosed, made available or otherwise used for purposes other than those specified, except with the consent of the data subject or by the authority of law.*

---

[8] NIST Special Publication 800-63: FAQ, Q-B10, https://pages.nist.gov/800-63-FAQ/#q-b10
[9] NIST Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf

ALA Privacy and Confidentiality Q&A[10]

3. What is explicit consent and how is it different from opt-out? 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.

21. Can circulation or registration information be used for other library purposes, such as to generate mailing lists for fund-raising by the library or its Friends group? The Fair Information Practice Principles of "Notice and Openness" and "Choice and Consent" should be reflected in library privacy policies. See "How to Draft a Library Privacy Policy."

Some states impose restrictions on the use of personally identifiable information (PII) for any purposes other than circulation or administration. In other states it is illegal to provide library user PII to any third party except under court order. See "State Privacy Laws Regarding Library Records." In all states, regardless of the status of the law, library policies regarding the collection, use and dissemination of PII should be carefully formulated and administered to ensure that they do not conflict with the ALA Code of Ethics that states "we protect each user's right to privacy and confidentiality." Libraries choosing to use PII for any library-related purpose other than for which the PII was gathered should consider the following standard "opt-in" practices:

- *Notice should be provided to all users of any library use of PII.*
- *Any use of PII beyond circulation or administration should be authorized only on an opt-in basis. At the time of registration, users should be asked to opt-in to additional and specifically enumerated uses of their PII (e.g., for fund-raising appeals). The PII of those who decline to 'opt-in' should not be made available for any additional uses.*

- *Any time a library decides to extend use of PII in ways not already authorized, it must seek user opt-in. Libraries should presume that all non-responders wish to opt out of the new use.*

22. Does the library's responsibility for user privacy and confidentiality extend to licenses and agreements with outside vendors and contractors? Most libraries conduct business with a variety of vendors in order to provide access to electronic resources, to acquire and

---

[10] ALA, Privacy and Confidentiality Q&A, http://www.ala.org/advocacy/intfreedom/privacyconfidentialityqa

run their automated systems, to offer remote storage (e.g., "cloud computing), or to enable access to the internet. Libraries need to ensure that contracts and licenses reflect their policies and legal obligations concerning user privacy and confidentiality. Whenever a third party has access to personally identifiable information (PII), the agreements need to address appropriate restrictions on the use, aggregation, dissemination, and sale of that information, particularly information about minors. In circumstances in which there is a risk that PII may be disclosed, the library should warn its users and/or discontinue use of that service. In addition, all library vendors and contractors that handle PII should be expected to maintain a publicly available privacy policy that commits to compliance with the NISO Consensus Principles on User's Digital Privacy in Library, Publisher, and Software-Provider Systems.

NISO (National Information Standards Organization): NISO Consensus Principles on User's Digital Privacy in Library, Publisher, and Software-Provider Systems (NISO Privacy Principles)[11]

3. Security: The most current security best practices should be used as the baseline to protect data. These should include encryption of personal data while they are at-rest and in-motion; prompt updates of systems and software to address vulnerabilities; systems, procedures, and policies for access control of sensitive data; a procedure for security training for those with access to data; and documented procedures for breach reporting, incident response, and system, software, and network security configuration and auditing.

Unauthorized access to user data should be remedied in a timely manner in order to minimize exposure of such data and affected parties should be informed as soon as is practicable in compliance with applicable laws. Libraries, content-, and software providers should comply with applicable statutory or regulatory requirements and published security standards intended to promote the privacy and security of user data.

4. Data Collection and Use: The potential benefit to the user, the library, content-, or software-provider derived from the collection and use of users' personal data must be

balanced against the impact of that collection and use on users and their right to privacy. Collection and use of users' personal data should be for the purposes of supporting user services, research to improve those services, or for the internal operations of the library, content-, or software-provider for which the data were gathered. The effective management and delivery of library services may require the library user to opt into the provision of personal data in order to access a library resource or receive library services. Users' personal data should only be used for purposes disclosed to them and to which they consent.

6. Options and Informed Consent: Each library user's needs and expectations of privacy are different and may be contingent on circumstances. When personal data are not required to

---

[11] NISO Consensus Principles on User's Digital Privacy in Library, Publisher, and Software-Provider Systems, https://groups.niso.org/apps/group_public/download.php/16064/NISO%20Privacy%20Principles.pdf

provide services as described in "Data Collection and Use", libraries and content- and software-providers should offer library users options as to how much personal information is collected from them and how it may be used. The default approach/setting should be that users are opted out of library services until they explicitly choose to opt in. In cases where a user opts in to a specific service, they should have the choice to opt out at a later date, in particular when privacy policies change, and at that time have the option to delete data as outlined in "Access to One's Own User Data" (item 10 below).

7. Sharing Data with Others: Libraries, content-, and software-providers sometimes need to share some data to provide content or library services, or undertake administrative functions. However, these parties must carefully consider the impact on the user's privacy before sharing data or information about their activity with third parties. Such considerations should include: the library user's consent; the user's privacy interests; any legal prohibitions or requirements; the policies of that third party and their adherence to these principles; and the risks and benefits to the user and institution.

User activity data to be shared should be anonymized and aggregated to a level that minimizes privacy risks to individual users, unless the user has opted-in to a service. In particular, possible exposure of the resource-use habits of individual users should be protected in conformance with the "Anonymization" principle (item 5 above).

Office of the New York State Comptroller Binghamton City School District – Information Technology (2019M-147)[12]

Audit Objective

Determine whether the Board and District officials adequately safeguarded data from abuse or loss.

Key Findings

- *Officials do not regularly review network user accounts and disable those that are determined to be unnecessary.*
- *The Board does not have an adequate contract and separate service level agreement (SLA) for information technology (IT) services provided by the Broome Tioga Board of Cooperative Educational Services' South Central Regional Information Center (SCRIC).*
- *Officials do not provide periodic IT security awareness training to staff.*

---

[12] Office of the New York State Comptroller, Binghamton City School District – Information Technology (2019M-147), https://www.osc.state.ny.us/local-government/audits/school-district/2019/10/25/binghamton-city-school-district-information-technology-2019m-147

- *In addition, sensitive IT control weaknesses were communicated confidentially to district officials.*

Key Recommendations

- *Regularly review user accounts and disable those that are unnecessary.*
- *Ensure there is an adequate contract and separate SLA with SCRIC for IT services provided.*
- *Provide periodic IT security awareness training to personnel who use IT resources.*

District officials generally agreed with our recommendations and indicated they planned to initiate corrective action.

Frequently Asked Questions Regarding Systems Access Policy

Are we able to get a mailing list of our library's patrons from the OWWL Library System so we can solicit donations?

The Systems Access and Confidentiality of Library Records Policy prohibits this use of patron data. The policy requires that patron data stored in Information Systems maintained by the OWWL Library System, like Evergreen, be used only for the purposes of providing library services to patrons. Any use of data from Evergreen should only be used for providing library services and cannot be exported or otherwise used for soliciting donations.

We've previously requested Evergreen data from the OWWL Library System to use to maintain our mailing list. What should we do if we're no longer able to request exports of our patron list?

The OWWL Library System follows ALA principles and guidelines in its implementation of a policy of not providing patron data for mailing lists used to solicit donations. The ALA recommends that patrons should be given the opportunity to opt-in to the use of their data for purposes beyond what is needed for providing library services.

Libraries who need to maintain a mailing list may want to consider modifying their registration workflows in a way that respects the principles described by the ALA. For example, libraries could add a section to their registration forms allowing patrons to opt-in to their data being added to a third-party service for the purpose of soliciting donations. Then, the patron's information could be added directly to the third-party platform your library uses for its mailing lists. This option is an informed opt-in: The patron should be informed of how their information will be used and that it will be stored in and processed by additional third-party platforms. This option would not require the use of data from Evergreen or other OWWL Library System-maintained systems.

What about a list of our patrons' email addresses? Can we request those to sign our patrons up for our newsletter? We let our patrons know that they will be automatically signed up when they register.

This is not an acceptable use of patron data according to the Systems Access and Confidentiality of Library Records Policy. Patrons should be given the opportunity to opt-in to use of their data,

especially if this data is being exported to a third-party newsletter platform. Furthermore, we cannot export patron lists in a way that includes only patrons who have opted-in to receiving your newsletter; we do not have an appropriate way to distinguish between patrons who have opted-in and those who have not.

What types of patron data requests can the OWWL Library System fulfill?

We are happy to fulfill a variety of different requests that rely on patron data.

For example, 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 data of birth (though we are happy to help you automate this change).

How can library staff protect patron data?

Upholding the information in this policy is critical for protecting patron data. A few points to remember: patron data should only be used for automated library notifications regarding available holds, checkouts, renewals, overdue materials, and card expirations. Staff may also directly communicate with a patron about issues with their account.

When discussing Information with other employees during your work, you should keep the conversation private and not overheard by others who are unauthorized to access such information. New York Law protects patron data and forbids the disclosure of library usage data. Discussing a book someone has checked out with unauthorized personnel can be considered a breach of that law and this policy.

It would also be prohibited by New York Law to discuss patron information or data with any unauthorized individual other than the patron on the account. This includes law enforcement without a proper warrant or court order.

Amended: November 8, 2023; June 14, 2023; April 12, 2023;
February 8, 2023; June 8, 2022
Adopted: September 8, 2021