Privacy in Your Library: Law, Ethics, and Policy  
PLA Conference 2016

I. Privacy in the Library

A. “In a library (physical or virtual), the right to privacy is the right to open inquiry without having the subject of one’s interest examined or scrutinized by others.” Privacy: An Interpretation of the Library Bill of Rights

B. “Confidentiality exists when a library is in possession of personally identifiable information about users and keeps that information private on their behalf.” Privacy: An Interpretation of the Library Bill of Rights.

C. Key concept: Privacy is essential to free inquiry in the library because it enables library users to select, access, and use information without fear of embarrassment, judgment, surveillance, punishment, or ostracism. If library users are to be truly free to make individual choices about what they read and view, they must have a reasonable expectation that their library use will be kept confidential.

II. Librarians and the Professional Obligation to Protect Patron Privacy

A. Article III, ALA Code of Ethics: "We protect each library user’s right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired or transmitted."

B. The Library Bill of Rights / Privacy: An Interpretation of the Library Bill of Rights: "The American Library Association affirms that rights of privacy are necessary for intellectual freedom and are fundamental to the ethics and practice of librarianship." See also Questions and Answers on Privacy and Confidentiality.

C. IFLA Statement on Libraries and Intellectual Freedom: "Library users shall have the right to personal privacy and anonymity. Librarians and other library staff shall not disclose the identity of users or the materials they use to a third party." See also the IFLA Statement on Privacy in the Library Environment.
D. **ALA Policy Concerning Confidentiality of Personally Identifiable Information about Library Users**

1. Assuring library users’ confidentiality is the primary means of providing library users with the kind of privacy that frees the user from the fear that he or she will experience retaliation or intimidation as a result of reading a book, viewing a website, or consulting another library resource.

2. Confidentiality extends to “information sought or received and resources consulted, borrowed, acquired or transmitted” (ALA Code of Ethics), and includes, but is not limited to, database search records; reference interviews; circulation records; interlibrary loan records; and other personally identifiable uses of library materials, facilities, or services.

E. **ALA Policy on the Confidentiality of Library Records**

1. “Libraries should formally adopt a policy that specifically recognizes its circulation records and other records identifying the names of library users to be confidential."

2. “Records shall not be made available to any agency of state, federal, or local government except pursuant to such process, order or subpoena as may be authorized under the authority of, and pursuant to, federal, state, or local law.”

F. **Key Concept:** Everyone (paid or unpaid) who works for the library in any capacity has an ethical obligation to not disclose a user's information without the user's consent. No one who works in the library should share personally identifiable user information or information about a user’s use of library resources with any third party (including family members, vendors, “Friends of the Library” groups, and law enforcement) unless given permission to do so by the user or required to do so by a court order.

III. **Laws That Protect Library Users’ Privacy**

A. **The U.S. Constitution and Readers’ Privacy**

1. The First Amendment protects the right to read and receive ideas anonymously, without government intrusion or observation.
2. The Fourth Amendment protects “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.”

3. Opinions issued by the U.S. Supreme Court and other federal and state courts both recognize and protect the right to read and receive ideas anonymously.

4. Key Concept: The First Amendment protects the privacy of a person’s reading habits, associations, and communications as an additional right necessary to give full meaning to the First Amendment’s enumerated rights of speech, press, belief, and assembly.

B. State Law and Library Users' Privacy

1. In 48 states and the District of Columbia, circulation records and records containing library users’ registration information are confidential and are exempt from disclosure to third parties.

   a. "Circulation record" includes all information identifying the individual’s use of particular books or materials.

   b. "Registration record" includes the information the library requires the individual to provide to the library in order to borrow or use library resources or materials.

   Example: Kansas

   K.S.A § 45-221(23): "Except to the extent disclosure is otherwise required by law, a public agency shall not be required to disclose library patron and circulation records which pertain to identifiable individuals."

2. Many states forbid disclosure of library records to third parties unless the library is presented with a valid court order authorizing the release of the information.

   Example: Minnesota
Private data; library borrowers.

(a) Except as provided in paragraph (b), the following data maintained by a library are private data on individuals and may not be disclosed for other than library purposes except pursuant to a court order:

(1) data that link a library patron’s name with materials requested or borrowed by the patron or that link a patron’s name with a specific subject about which the patron has requested information or materials; or

(2) data in applications for borrower cards, other than the name of the borrower.

3. Key Concept: States recognize an individuals’ right to privacy in records of their library use, and that library users should have a reasonable expectation that records of their library use will be kept confidential. Librarians, trustees, and library staff should consult with local legal counsel to determine their rights and responsibilities under state law.

IV. Ensuring Privacy and Confidentiality for Library Users
(See, generally, the ALA-IFC Privacy Toolkit).
A. Privacy Policy Fundamentals

1. Well-defined privacy policy statements should communicate the library’s commitment to protecting users’ personally identifiable information, inform library users how their personally identifiable information is used, stored, and protected by the library, and explain under what circumstances personally identifiable information might be disclosed to third parties and law enforcement.

2. Supplemental policies set forth library policy and procedure concerning records retention and records management and provide guidelines to library employees when responding to outside inquiries concerning user records, including inquiries from law enforcement agents.
3. Written policies and procedures serve to provide documentary evidence of library practice and intent in regards to user privacy, records management, and library procedure.

4. State open records laws, local ordinances addressing open records and records management, and state Freedom of Information Acts all must be considered when devising policies concerning the management of library records.

B. **Fundamental Privacy Procedures**

1. Avoid creating unnecessary records.

2. Avoid retaining records that are not needed for efficient operation of the library, including data-related logs, digital records, vendor-collected data, and system backups.

3. Limit the degree to which personally identifiable information is monitored, collected, disclosed, and distributed.

4. Avoid library practices and procedures that place personally identifiable information on public view.

5. Employ robust encryption and cybersecurity measures to protect user data and endeavor to store it on servers maintained by library.

6. When user data is provided to, or managed by, a vendor providing e-content, cataloging, and data management services to the library, the library should require the vendor to enter into a legal agreement with the library that stipulates that the library retains control of its users’ data, that the data is confidential, and that it may not be used or shared with third parties except with the permission of the library.

7. **Key Concept:** Libraries should minimize the collection of personally identifiable user information, store it locally and securely, maintain legal control of the data and insure that library practices do not divulge user information or put it on public view (e.g., self-service hold shelves that reveal a user’s identity).

C. **Records Management Policy**
1. Personally identifiable information should be regularly purged, including personally identifiable information associated with library resource use, material circulation history, and security/surveillance tapes and logs.

2. "Purging" does not imply wholesale destruction of records. Statistical information, library usage data permanently stripped of personally identifiable information, and historical documents can and should be retained to aid library administration and preservation of the historical record.

3. Policies addressing records management, including purging, must be employed throughout the institution, including information technology departments and off-site locations.

4. Physical records containing users' personally identifiable information or financial information should be secured and kept from public view while needed and shredded when no longer needed.

D. Other Elements of Privacy in the Library

1. Observation

   a. Even though libraries are public places, libraries, and those who work for libraries, should strive to protect users’ privacy when they are using library resources, whether print or online.

   b. Carrels, stacks, and computer stations should be arranged in a manner that discourages or prevents someone reading over a user's shoulder without the user being aware of the activity.

   c. Reference desks should be arranged so that a user can ask a question in confidence without being overheard.

   d. Libraries that use surveillance cameras should have written policies stating that the cameras are not to be used for any other purpose than security.
1. Avoid placing cameras in a manner that records what users are reading, viewing, or checking out.

2. If the cameras create records via film, tape, or electronic files, the library must recognize its responsibility to protect the confidentiality of those records like any other library record, including purging the records as soon as their purpose is served.

2. Anonymity

   a. "The right to open inquiry without having the subject of one’s interest examined or scrutinized by others" includes the ability to use library resources anonymously.

   b. Anonymity is an important factor in providing equity of access to information, particularly for those who are members of especially vulnerable groups.

   c. Where possible and feasible, allow the use of pseudonyms, aliases, guest log-ins, anonymizing software and community terminals for those who request them.

   d. Where anonymity is not possible, provide information about the library’s commitment to confidentiality.

*These materials are not a legal opinion nor should they be regarded as legal advice. Readers should consult their own legal counsel for legal advice regarding their particular situation.*

Prepared by:
Deborah Caldwell-Stone
Deputy Director
ALA Office for Intellectual Freedom
April 2016
American Library Association
Please do not publish or distribute without permission
Questions about these materials may be directed to the
ALA Office for Intellectual Freedom at oif@ala.org
Library Privacy Guidelines for E-book Lending and Digital Content Vendors

Introduction

Protecting user privacy and confidentiality has long been an integral part of the intellectual freedom mission of libraries. The right to free inquiry as assured by the First Amendment depends upon the ability to read and access information free from scrutiny by the government or other third parties. In their provision of services to library users, librarians have an ethical obligation, expressed in the ALA Code of Ethics, to preserve users’ right to privacy and to prevent any unauthorized use of patron data[1]. Librarians and libraries may also have a legal obligation to protect library users’ data from unauthorized disclosure.

Libraries enter into licenses or agreements with commercial vendors in order to provide library users access to digital information, including e-books, journals, and databases. Access to these resources is most often provided via networks and the internet. In the course of providing these services, most e-book and digital content vendors collect and use library patron data for a variety of reasons, including digital rights management, consumer analytics, and user personalization. Libraries and vendors must work together to ensure that the contracts and licenses governing the provision and use of digital information reflect library ethics, policies, and legal obligations concerning user privacy and confidentiality.

These guidelines are issued to provide vendors with information about appropriate data management and security practices in respect to library patrons' personally identifiable information and data about their use of digital content.

Agreements, Ownership of User Data, and Legal Requirements

Agreements between libraries and vendors should address appropriate restrictions on the use, aggregation, retention, and dissemination of patron data, particularly information about minors. Agreements between libraries and vendors should also specify that libraries retain ownership of all data and that the vendor agrees to observe the library's privacy policies and data retention and security policies.

Vendors are strongly encouraged to implement the principles of privacy by design, i.e. products and services should have privacy concerns “built in, not bolted on.” In addition, agreements between libraries and vendors should reflect and incorporate restrictions on the potential dissemination and use of library patrons' records and data
imposed by local, state, and federal law.

**Clear Privacy Policies**

Library users should be notified about vendor privacy policies when accessing a product or service. The privacy policies should be made easily available and understandable to users. Safeguarding user privacy requires that individuals know what information is gathered about them, how long it is stored, who has access to it and under what conditions, and how it is used. There should be a way to actively notify ongoing users of any changes to the vendor’s privacy policies.

**User Consent**

The vendor should give users options as to how much personal information is collected from them and how it may be used. Users should have choices about whether or not to opt-in to features and services that require the collection of personal information. Users should also have the ability to opt-out and have their personal information erased if they later change their minds.

**Access to Personal Data**

Users should have the right to access their own personal information and contest its accuracy. Verifying accuracy helps ensure that vendor services that rely on personal user information can function properly. Guidance on how the user can access their personal data should be clear and easy to find. Patrons should also have the ability to download their personal data into an open file format such as CSV for their own use.

Access to personal information should be restricted to the user and conform to the applicable state laws addressing the confidentiality of library records as well as other applicable local, state, and federal law.

**Data Integrity and Security**

Whenever patron data is collected, the vendor must take reasonable steps to ensure integrity and security, including compliance with applicable statutory requirements.

**Security:** Security involves both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of data. Security measures should be integrated into the design, implementation, and day-to-day practices of the vendor’s entire operating environment as part of its continuing commitment to risk management. The vendor should seek compliance with published cybersecurity standards from organizations such as National Institute of Standards and Technology (NIST).

**Encryption:** The use of data encryption helps enhance privacy protection. All online transactions between client applications (web browsers, mobile apps, etc.) and server applications should be encrypted. In addition, any user data housed by the vendor off site (cloud-based infrastructure, tape backups, etc.) should use encrypted storage.

**Anonymization:** Data used for customer analytics and other types of analysis should be anonymized by removing or encrypting personally identifiable
information. While data anonymization is a good practice, it is not foolproof (re-identification analysis has been used to identify individuals from anonymized data sets); therefore access should still be restricted.

Retention: User data should not be retained in perpetuity. The vendor should establish policies for how long to retain different types of data and methods for securely destroying data that is no longer needed. For example, accounts that are expired or inactive for a certain amount of time should be purged. Retention policies should also cover archival copies and backups.

Data Sharing: User data should not be shared with third-party vendors and other business associates without user consent. Most state statutes on the confidentiality of library records do not permit release of library patrons’ personally identifiable information or data about their use of library resources and services without user consent or a court order. In addition, ALA policy forbids sharing of library patron information with third parties absent a court order.

Government Requests: The vendor should develop and implement procedures for dealing with government and law enforcement requests for library patrons’ personally identifiable information and use data. The vendor should consider a government or law enforcement request only if it is issued by a court of competent jurisdiction that shows good cause and is in proper form. The vendor should inform and consult with the library when it believes is obligated to release library patrons' information unless prevented from doing so by the operation of law. The vendor should also inform users through its privacy policies about the legal conditions under which it might be required to release personally identifiable information.

Company Sale, Merger, or Bankruptcy: In the event that the vendor is sold to another company, merges with another company, or is dissolved through bankruptcy, all personally identifiable information should be securely destroyed, or libraries and their end users must be notified and given the opportunity to request that their data be securely destroyed.

User Devices

Privacy protections for library patrons' personally identifiable information and use data should extend to the user's device, including the web browser or any applications provided by the vendor. All communications between the user's device and the vendor's services should be encrypted. If the vendor wishes to employ personalization technology such as persistent cookies on its website or allows third-party web tracking, it should inform the user and give them the chance to opt-in before initiating these features for the user. If a vendor-provided application stores personally identifiable information or use data on the user's device, it should be encrypted. The user should be able to remove a vendor-provided application and delete any data stored on the device.

Audit and Notification

Vendors should establish and maintain effective mechanisms to enforce their privacy
policies. They should conduct regular privacy audits to ensure that all operations and services comply with these policies. The results of these audits should be made available upon request to libraries that are customers or potential customers. A vendor that suffers a breach in its privacy policies through inadvertent dissemination or data theft must notify the effected libraries and users about this urgent matter as soon as the vendor is aware of the data breach.

Approved by the Intellectual Freedom Committee 6/29/2015

[1] Patron data" or "user data" is any data or record that identifies the library patron or the patron's use of library information systems and resources.
NISO Consensus Principles on User’s Digital Privacy in Library, Publisher, and Software-Provider Systems
(NISO Privacy Principles)

Published on December 10, 2015
About NISO Principles
Developed by the members of the National Information Standards Organization (NISO), NISO principles provide general guidance on an area of concern and are intended to advance community discussions and thought on developing issues. As the issues are still emerging when the principles are released, the language is not voted upon or approved by NISO’s members or Topic Committees. Future work by NISO or others may provide normative language related to the issues described in these principles. For current information on the status of this publication contact the NISO office or visit the NISO website (www.niso.org).

ISBN 978-1-937522-70-4

Published by
National Information Standards Organization (NISO)
3600 Clipper Mill Road
Suite 302
Baltimore, MD 21211
www.niso.org

This work is licensed under a Creative Commons Attribution Share-Alike version 4.0 License.
The National Information Standards Organization (NISO) wishes to thank the many individuals representing various groups within the information community whose efforts helped to develop these privacy principles. Their high-level work on balancing the privacy needs and expectations of library patrons with the operational needs of libraries and library vendors is invaluable.

**Steering Committee**

**Daniel Ayala**  
*Director, Global Information Security*  
*ProQuest*

**Peter Brantley**  
*Director, Digital Library Applications*  
*The New York Public Library*

**Marshall Breeding**  
*Consultant*  
*Library Technology*

**Todd Carpenter**  
*Executive Director, NISO*  
*Principal Investigator*

**Eric Hellman**  
*President*  
*Gluejar*

**Lisa Hinchliffe**  
*Professor/Coordinator for Strategic Planning*  
*Coordinator for Information Literacy Services & Instruction*  
*University of Illinois at Urbana-Champaign*

**Nettie Lagace**  
*Associate Director for Programs*  
*NISO*

**Bonnie Tijerina**  
*Fellow*  
*Data & Society Research Institute*

**Michael Zimmer**  
*Associate Professor, University of Wisconsin-Milwaukee*  
*Director of the Center for Information Policy Research*
Core Working Group
IJJsbrand Jan Aalbersberg, Elsevier
Micah Altman, Massachusetts Institute of Technology Libraries
Daniel Ayala, ProQuest
Lori Bowen Ayre, The Galecia Group
Peter Brantley, University of California, Davis Library
Marshall Breeding, Independent consultant, Speaker, and Author
Deborah Caldwell-Stone, Office for Intellectual Freedom, American Library Association
Todd Carpenter, NISO
Galen Charlton, Equinox Software, Inc.
Richard Entlich, Cornell University Library
Eric Frierson, EBSCO Information Services
David Greene, Electronic Frontier Foundation
Kathryn Harnish, ProQuest
Christopher Harris, School Library System of the Genesee Valley Educational Partnership
Eric Hellman, Gluejar
Lisa Hinchliffe, University Library, University of Illinois at Urbana-Champaign
David Lee King, Topeka & Shawnee County Public Library
Nettie Lagace, NISO
Cliff Lynch, Coalition for Networked Information
Alison Macrina, Library Freedom Project
Peter Murray, The Cherry Hill Company
Bobbi Newman, Speaker, Writer, Trainer, Consultant
Andrew Pace, OCLC
Gary Price, Library Journal's INFOdocket and FullTextReports.com
Laura Quilter, University of Massachusetts Amherst Libraries
Michael C. Robinson, University of Alaska Anchorage/Alaska Pacific University Consortium Library
Alan Rubel, University of Wisconsin at Madison
Shlomo Sanders, Ex Libris
Roger Schonfeld, ITHAKA
Michael Taylor, Elsevier
Bonnie Tijerina, Data & Society Research Institute
Michael Zimmer, Center for Information Policy Research, University of Wisconsin-Milwaukee
Ken Varnum, University of Michigan Library
Abigail Wickes, University of Oxford Press
Mei Zhang, University of Wisconsin at Madison
NISO Consensus Principles on Users’ Digital Privacy in Library, Publisher, and Software-Provider Systems (NISO Privacy Principles)

Preamble
Support of intellectual freedom and protection of user privacy and user confidentiality have long been integral components of the missions of libraries and related institutions. The management of information resources increasingly involves digital networks that, by their nature, include possibilities for tracking and monitoring of user behavior, whether content or services delivered are physical or digital. As this ecosystem of electronic systems to manage library-supplied resources has grown and expanded beyond the library’s internal operations, the larger community of libraries, content-, and software-providers needs to recognize the implications this has on users’ privacy. Libraries, publishers, and software-providers have a shared obligation to foster a digital environment that respects library users’ privacy as they search, discover, and use those resources and services.

Certain personal data are often required in order for digital systems to deliver information, particularly subscribed content. Additionally, user activity data can provide useful insights on how to improve collections and services. However, the gathering, storage, and use of these data must respect the trust users place in libraries and their partners. There are ways to address these operational needs while also respecting the user’s rights and expectations of privacy.

Information management practices, security protocols, and legal frameworks evolve over time, and that evolution has implications for user privacy. It is therefore incumbent on all participants in the information ecosystem to strive toward continuous improvement of their activities and policies to ensure the most appropriate level of protection for users’ personal data.

The principles outlined in this document are a starting point. Additional community consensus work will be necessary to make some of these principles implementable by the spectrum of providers that supports library services. We encourage all those involved in provision of library-user services to contribute to future work related to the themes covered below.

Through the following principles, we strive to encourage consensus around practices and procedures that protect the digital privacy of the library user.
1. Shared Privacy Responsibilities
As expressed in these principles, the ALA Code of Ethics, and the IFLA Code of Ethics, libraries and librarians have an ethical obligation—and in some cases a legal obligation—to preserve users’ privacy and to prevent any unauthorized collection, use, or disclosure of library users’ data. Publishers and software-providers, which operate through and for the library and its users, share in this ongoing ethical responsibility. Anyone with access to library data and activity should accept responsibility for safeguarding user privacy and data security and should have training in related standards and best practices.

2. Transparency and Facilitating Privacy Awareness
Library users need to be able to determine the extent of privacy protections provided and the boundaries of those protections as they use library resources. Libraries, content-, and software-providers shall make readily available to users specific, non-technical statements that describe each stakeholder’s policies and practices relating to the management of personally identifiable information. These policies should also inform library users how they can protect the privacy of their data themselves. Such statements shall identify what data are collected, why data is collected, who has access to the data, how the data are stored and secured, when that data might be disclosed and to whom, and what the organization’s data retention and/or deletion policies are.

Library users can best take advantage of the privacy protections afforded by libraries if they understand the extent to which their privacy is and/or is not protected. Means of communicating privacy choices to users include outreach, inclusion of library-user communication methods in systems design, and user education. All parties involved in providing services should effectively communicate those choices to users. Systems should be designed in a way that facilitate understanding of policies through the use of simplified management of options.

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.

Certain types of personal data (e.g., regarding race, gender, socioeconomic class, ability, etc.) are perceived to be more sensitive, and if they are to be held or used by a library, content-, or software-provider, should require higher levels of scrutiny and justification. In addition, such data require extra protection once they are collected.

5. Anonymization
That portion of library user data that includes personally identifiable information should be retained in that form only as long as absolutely necessary for operational purposes. After operational needs expire, if data are to be retained for research purposes or in support of administrative objectives, personally identifiable information should be masked through anonymization processes unless users have consented to retention of personally identifiable information. Anonymization should be used as part of a broad set of information privacy controls that include: data minimization; statistical disclosure limitation methods, such as controlled aggregation; data-use agreements; and auditing. Anonymization may not completely eliminate the risk of re-identification. Therefore even anonymized raw data should be treated with the precautions detailed in the Security principle (item 3 above), in proportion to the potential risk of re-identification.

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 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).

To support the policies outlined in the “Transparency” section (item 2 above), privacy policies should be made easily available and understandable to users. These policies might change over time, so providers of library services should publish notice of any significant changes to their privacy policies, and there should be an effort to directly notify impacted users of any changes to the library’s or vendor’s privacy policies. Changes to policies should not be applied retroactively to user data without users’ consent except as required by law.

9. Supporting Anonymous Use
Libraries and content- and software-providers must recognize the right of library users to be anonymous, should they so choose, and users should be provided appropriate affordances. Not all service capabilities may be available while a user remains
anonymous, but reasonable accommodations to provide basic services should be made. When the collection and retention of a user’s personal data are required in order to access library resources or deliver library services, the library user should be informed that anonymous service is not possible.

10. Access to One’s Own User Data
Users should have the right to access their own personal information or activity data. Users should be provided, in so far as is feasible, access to these data for review, so that users may request correction or deletion. Organizations holding these data should make their best effort to provide it. Some records may not be able to be deleted if they are required by the library, content-, or software-provider for internal operations or business purposes as described in “Data Collection and Use” (item 4 above). As an optional service, providers might make these data securely exportable in common file formats.

11. Continuous Improvement
Libraries, content-, and software-providers should continuously assess and strive to improve user privacy as threats, technology, legal frameworks, business practices and user expectations of privacy evolve.

12. Accountability
Libraries, content-, and software-providers should establish a culture of accountability in which data collection, security, use, sharing, and disposal practices and policies are reviewed and reported on a periodic basis. Accountability practices will evolve over time, but they should include, where appropriate, periodic reviews or audits of computer systems, security practices, policies, and procedures, preferably by independent third parties. The conclusions of reviews or audits should be available to libraries on request.
Glossary

**Anonymization**: The process of transforming or removing personally identifiable information from data sets, so that the people whom the data describe remain anonymous.

**ALA**: American Library Association

**Content provider**: Any entity that provides content to library users under an agreement with the library. An entity can simultaneously be both a content- and a software- (or systems-) provider.

**Data at-rest, data in-use, and data in-motion**: Terms describing the status of personally identifiable information or personal activity data housed within library, content- or software-provider infrastructure. Data at-rest describes data while it is stored within systems. Data in-use means data that is being processed or used to provide a service. Data in-motion is data that is being transferred for storage or processing.

**Informed Consent**: An individual’s ability, based on access to information in privacy policies, to determine whether or how their personal information may be used or disclosed by the entity that collected the information.

**IFLA**: International Federation of Library Associations and Institutions.

**Internal operations**: Business or administrative processes or activities undertaken to provide, maintain, improve, or support core objectives of the organization.

**Library services**: The activities a library either directly provides, enables, or hosts, or contracts with an outside organization to provide, enable, or host, that support the mission of the library and assist the patron or user of library resources.

**Library user**: Anyone who avails of library services, materials, or systems. This includes patrons, library staff, volunteers, and any other community member accessing library resources or services.

**Software provider**: Any entity that provides digital systems and/or services that facilitate the management, discovery, delivery, use, or preservation of library owned or licensed resources. An entity can simultaneously be both a library, a content- and a software- (or systems-) provider.

**Personal activity data**: Data that is generated by a library user’s activity in a library context that can be traced to that individual. Examples include circulation records, search, browsing and download history, social media interactions, online communications history (e.g., email, SMS, etc.), library activity logs, reading behavior data, authentication logs, and computer-use data.
Personally identifiable information (PII): Data that can be used—on their own or in combination with other data—to identify, contact, or locate a single person, or to identify that individual in context. Also called personal information.

Privacy: As defined by National Research Council and the Social Science Research Council; “Informational privacy encompasses an individual’s freedom from excessive intrusion in the quest for information and an individual’s ability to choose the extent and circumstances under which his or her beliefs, behaviors, opinions, and attitudes will be shared with or withheld from others.” (Report of the National Academy of Science 1993 Panel Report Private Lives and Public Policies, p. 22) There are many other definitions of privacy in an information environment and there is no consensus about all the elements that privacy covers.

Privacy policies: The public description of the processes and practices that outline how an organization gathers, uses, discloses, and manages personally identifiable information and personal activity data.

Third-parties: Entities that are neither libraries, content providers, nor systems providers and who are not directly tied to the operational provision of services to the library user.

Related Reading

ALA Code of Ethics
http://www.alaa.org/advocacy/proethics/codeofethics/codeethics

IFLA Code of Ethics

The creation of these principles was funded by a generous grant from the Andrew W. Mellon Foundation.
**Example of Privacy Policy and Notice Addressing Data Use**

Privacy and confidentiality of library records
Multnomah County Library

Last revised 05.07.2015

Policy summary

This privacy policy explains your privacy and confidentiality rights and responsibilities, the steps Multnomah County Library takes to respect and protect your privacy when you use library resources, and how we handle personally identifiable information we collect from our patrons. Multnomah County Library has measures in place to protect patron privacy and confidentiality. In setting these policies, the library tries to strike a balance between your privacy and your convenience. Third party services provided through the library have other terms and policies that affect the privacy of your personally identifiable information. Patrons must understand when accessing remote or third party vendor sites that there are limits to the privacy protection the library can provide. Links to the terms and policies of many of the library's third-party vendors are provided below.

Please ask a staff member if you have questions about this policy. We're here to help.

Introduction

Multnomah County Library takes steps to protect the privacy and confidentiality of all library patrons, no matter their age. Our commitment to your privacy and confidentiality has deep roots not only in the law but also in the ethics and practices of librarianship. In accordance with the American Library Association's Code of Ethics: "We protect each library user's right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired, or transmitted." Multnomah County Library's privacy and confidentiality policies are in compliance with applicable federal, state, and local laws.

State law protects your library records from disclosure if a member of the public or the media requests them. Library records include your circulation records, your name together with your address or telephone number, and your email address. Library records may be subject to disclosure to law enforcement officials under provisions of state law, the USA PATRIOT Act or in a civil lawsuit. Librarians may be forbidden from reporting to you that your records have been requested or obtained under provisions of the USA PATRIOT Act.

Privacy and confidentiality policy

We post publicly the library's privacy and information-gathering policies. We avoid creating unnecessary records, we avoid retaining records not needed for library business purposes, and we do not engage in practices that might place personally identifiable information on public view without your consent.

Information the library may gather and retain about library patrons includes the following:

- Information required to register for a library card or use the John Wilson Special Collections (e.g. name, address, telephone number, email address, birthdate)
- Records of material checked out, charges owed, payments made
- Records of electronic access information such as the library card or guest pass number used to log onto library public computers
- Requests for interlibrary loan or reference service
- Sign-up information for library classes, programs, Sterling Room for Writers
- Information about topics searched for (does not contain any personally identifiable information)
The library will not collect or retain your private and personally identifiable information without your consent. Individuals may choose to submit their names, email addresses, postal addresses or telephone numbers in order to receive library services, such as registering for library cards, ordering materials, receiving personal responses to questions or being added to specific mailing lists. If you consent to give us your personally identifiable information, we will keep it confidential and will not sell, license or disclose it to any third party, except those working under contract to the library, or except as required by law. For information about the ways third parties may use or disclose your information see the Third Party Vendor Services section below.

We never use or share the personally identifiable information provided to us in ways unrelated to the ones described above without also providing you an opportunity to prohibit such unrelated uses, unless we are required by law to do so.

Access to accounts and patron responsibility

Protecting Your Library Card

It is your responsibility to notify the library immediately if your card is lost or stolen or if you believe someone is using your card or card number without your permission. We encourage you to protect your PIN/password for your privacy and security.

Keeping Account Information Up-To-Date

You may access your personally identifiable information held by us and are responsible for keeping your information accurate and up-to-date. You may choose to use a preferred name in addition to your legal name. If you choose to use a preferred name, library correspondence will be addressed to your preferred name. Please ask a staff member if you have questions about the process for accessing or updating your information.

Parents and children

We respect the privacy of all library patrons, no matter their age. Parents, guardians or caretakers of a child under age 18 who wish to obtain access to a child’s library records, including the number or titles of materials checked out or overdue, must provide the child’s library card or card number.

Having other people help you with your account

You may have other people help you with your account by providing them with your library card or card number and PIN/password. Please ask a staff member if you have questions about the process for having others assist you with your account.

Items on hold

Items placed on hold for library patrons are shelved by the patron’s last name for pick-up in the public areas of our libraries. Patrons who do not want their holds shelved by last name may have their holds shelved by a unique user ID number (NOT the library card number). Patrons of any age may choose to have other people pick up their holds. Holds will be checked out on the library card presented at the time of check-out.

Data security

The library takes reasonable steps to assure data security. We protect personally identifiable information by electronically purging or manually shredding it once it is no longer needed for library business purposes, whenever possible. We have invested in appropriate technology to protect the security of personally identifiable information while it is in the library’s custody. We take steps to remove personally identifiable information from aggregate, summary data. We regularly remove cookies, browsing history, cached files, or other computer and Internet use records that are placed on our computers or networks.

Security measures
Our policies and procedures limit access to data and ensure that those individuals with access do not use the data for unauthorized purposes. We limit access through the use of strong passwords that are changed regularly and storage of data on secure servers or computers.

Staff may access personally identifiable information stored in the library’s computer systems only for the purpose of performing their assigned library duties. Staff will not disclose any personally identifiable information to any other party except where required by law or to fulfill your service request.

Cookies

A cookie is a small amount of data, which often includes a unique identifier that is sent to your computer or mobile phone or device browser from a website’s computer and is stored on your device’s hard drive. Each website can send its own cookie to your browser if the browser preferences you have set allow it. Many websites do this whenever a user visits their website in order to track online traffic flows. Websites also use cookies to customize your user experience to your preferences.

The library uses cookies to verify that you are an authorized user in order to allow access to licensed library resources, to customize Web pages for your use, to help make our site more useful to visitors and to learn about the number of visitors to our site and the types of technology our visitors use.

Some of the applications or external sites that you may link to from our pages, devices or equipment also use cookies. For more information on the use of cookies by each service please refer to the Terms of Use and Privacy Policies for the services you use. You may set the preferences in your web browser to refuse cookies or to tell you when a cookie is being sent. This may result in an inability to access some library services from computers outside the library.

Third party vendor services

Multnomah County Library enters into agreements with third parties to provide online services, digital collections, streaming media content and to improve our website. When using some of these services, you may also connect with social networks and other users of these services.

Third party services may gather and disclose your information, including,

- Personally identifiable information you knowingly provide, including when you register for the site, provide feedback and suggestions, request information or create shared content,
- Other information that could be used to identify you such as your IP address, search history, location based data and device ID,
- Non-personally identifiable information, such as your ad views, analytics, browser information (type and language), cookie data, date/time of your request, demographic data, hardware/software type, interaction data, serving domains, pageviews and the web page you have visited immediately prior to visiting the site, and
- Other data that third party services may collect as described in the vendor’s privacy policy and terms of use.

For more information on these services and the specific types of data that may be gathered and disclosed by each service please refer to the Terms of Use and Privacy Policies for the services you use. Links to our major vendors’ policies are provided here. You may choose to not use these third party services if you do not accept their Terms of Use and Privacy Policies; please read them carefully.

Policies for our discovery software for the on-line catalog:

- Bibliocommons (MyMCL)

Policies for our e-books, audiobooks, streaming music, movies, and kids’ stuff:

- 3M Cloud Library
- Alexander Street Press
- BookFlix
• eBrary and ProQuest products
• Ebsco
• Gale products
• Hoopla
• IndieFlix
• OverDrive
• OverDrive Kids
• StarWalk KidsMedia
• TumbleBook Library
• Zinio/Recorded Books

Policies for online help, including the Ask-A-Librarian and My Librarian text and email reference services:

• Answerland
• Knowledge Tracker
• Mollom
• Mosio

Policies for the services we use to improve our website:

• Google Analytics
• Score Card Research

Policies for our wireless printing service:

• Envisionware
• PrinterOn

Policy for our collections agency:

• Unique Management Services, Inc.

We make reasonable efforts to ensure that the library’s contracts, licenses, and off site computer service arrangements reflect our policies and legal obligations concerning user privacy and confidentiality. Our agreements address appropriate restrictions on the use, aggregation, dissemination, and sale of information, particularly information about minors. When connecting to licensed databases and content providers outside the library, we release only information that authenticates users as registered Multnomah County Library patrons.

Multnomah County Library expects vendors to

• abide by privacy related components of library/vendor contract and licensing agreements,
• conform to library privacy policies regarding the retention and release of information to third parties,
• provide a product which complies with the provisions of Children's Online Privacy Protection Act (COPPA), and
• refrain from collecting or disclosing additional information about patron activity or identifiers other than is needed for administration of the library service provided.

Nevertheless, patrons must understand when accessing remote or third party vendor sites that there are limits to the privacy protection the library can provide.
Other services

This privacy and confidentiality policy does not apply to external applications or websites that you may access from the library’s public computers, devices or equipment (such as Internet computers, Chromebooks and iPads).

Some patrons may choose to take advantage of RSS feeds from the library catalog, public blogs, hold and overdue notices via e-mail or text message, and similar services that send personally identifiable information related to library use via public communication networks. Patrons should also be aware that the library has limited ability to protect the privacy of this information once it is outside our control.

Illegal activity prohibited and not protected

Patrons may conduct only legal activity while using library resources and services. Nothing in this policy prevents the library from exercising its right to enforce its Rules of Behavior, protect its facilities, network and equipment from harm, or prevent the use of library facilities and equipment for illegal purposes. 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. Staff is authorized to take immediate action to protect the security of library patrons, staff, facilities, computers and the network. This includes contacting law enforcement authorities and providing information that may identify the individual(s) suspected of a violation.

Enforcement and redress

If you have a question, concern, or complaint about our handling of your personally identifiable information or this policy you may file written comments with the Director of Libraries. We will respond in a timely manner and may conduct an investigation or review of practices and procedures. We conduct such reviews regularly to ensure compliance with the principles outlined in this policy.

The Director of Libraries is custodian of library records and is authorized to receive or comply with public records requests or inquiries from law enforcement officers. The Director may delegate this authority to designated members of the library’s management team. The Director confers with the Office of the Multnomah County Attorney before determining the proper response to any request for records. We 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. We have trained all library staff and volunteers to refer any law enforcement inquiries to the Office of the Director of Libraries.
The Fair Information Practice Principles

To truly enhance privacy in the conduct of online transactions, Fair Information Practice Principles (FIPPs) must be universally and consistently adopted and applied in the Identity Ecosystem. FIPPs are the widely accepted framework of defining principles to be used in the evaluation and consideration of systems, processes, or programs that affect individual privacy.¹

In brief, the Fair Information Practice Principles are:

- **Transparency**: Organizations should be transparent and notify individuals regarding collection, use, dissemination, and maintenance of personally identifiable information (PII).

- **Individual Participation**: Organizations should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. Organizations should also provide mechanisms for appropriate access, correction, and redress regarding use of PII.

- **Purpose Specification**: Organizations should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

- **Data Minimization**: Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).

- **Use Limitation**: Organizations should use PII solely for the purpose(s) specified in the notice. Sharing PII should be for a purpose compatible with the purpose for which the PII was collected.

- **Data Quality and Integrity**: Organizations should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.

- **Security**: Organizations should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

- **Accountability and Auditing**: Organizations should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

Universal application of FIPPs provides the basis for confidence and trust in online transactions.

¹ Rooted in the United States Department of Health, Education and Welfare’s seminal 1973 report, “Records, Computers and the Rights of Citizens” (1973), these principles are at the core of the Privacy Act of 1974 and are mirrored in the laws of many U.S. states, as well as in those of many foreign nations and international organizations. A number of private and not-for-profit organizations have also incorporated these principles into their privacy policies. See, also guidance at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.