Guidelines and Resources
for Minors and Students in K-12 Schools

Library Privacy in a Digital Age

American Library Association Office for Intellectual Freedom

ALA American Library Association

Contents

Privacy Fundamentals

I. Privacy in the Library

A. "The right to privacy includes the right to open inquiry without having the subject of one's interest examined or scrutinized by others, in person or online." *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.*

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, 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 and not disclosed to third parties. These principles apply to all library users, regardless of their age, status, background, ethnicity, race, religion, or viewpoint.

II. Librarians and the Professional Obligation to Protect Patron Privacy

A. Article VII, ALA Library Bill of Rights: "All 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."

B. 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."

C. 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.

D. 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.

E. 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 because 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.

F. 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.”

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. These principles apply regardless of the age, status, background, ethnicity, race, religion, or viewpoint of the library user.

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.

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 : 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; 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.

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

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 regard 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.

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).

Records Management Policy

7. 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.

8. "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.

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

10. 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.

C. Observation

1. 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.

2. 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.

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

4. Libraries that use surveillance cameras should have written policies stating that the cameras are not to be used for any other purpose than security.

5. Avoid placing cameras in a manner that records what users are reading, viewing, or checking out from the library's resources.

6. 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.

D. Anonymity

1. 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.

2. Anonymity is an important factor in providing equity of access to information, particularly for those who are members of marginalized or especially vulnerable groups, including young people, persons of color, immigrants, and lesbian, gay, bisexual, transgender, and queer persons.
3. Where possible and feasible, allow the use of pseudonyms, aliases, guest logins, anonymizing software and community terminals for those who request them.

4. 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.

ALA Library Privacy Guidelines: Students in K – 12 Schools

Introduction
Libraries face a number of challenges in protecting the privacy of users, especially students in elementary, middle, and high schools. School libraries offer print, media, and online content to meet students' educational and research needs as well as to nurture their intellectual curiosity and development. Students' use of library resources is also incorporated into classroom activities, learning outcomes, and assessment.

School libraries typically are integrated into their district's administrative and technology infrastructures. Depending on district administration and outside cooperative technology or vendor agreements, school libraries have greater or lesser degrees of autonomy. A lack of autonomy may make it difficult for librarians

to implement policies and procedures to protect student privacy in regard to the use of library systems, applications, and collections. In addition, state and federal laws regarding library records, educational records (e.g., the Family Educational Rights and Privacy Act (FERPA), and the online activities of minors (e.g., the Child Online Privacy Protection Act (COPPA) have both positive and negative impacts on the privacy rights of students. For example, FERPA defines explicit rights to privacy for students and minors but at the same time grants schools and parents access to, and oversight over, student records that weakens these privacy rights.

ALA issues these guidelines to provide school libraries with information about appropriate data management and security practices in respect to student use of library collections and resources in order to strengthen student privacy protections.

Why Privacy Is Important

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. Librarians and libraries may also have a statutory or regulatory obligation to protect library users' personally identifiable information and data from unauthorized disclosure and use.

Students' and minors' First Amendment rights to free inquiry and privacy must be balanced against both the educational needs of the school and the rights of the parents. As students and minors mature, it is increasingly important that they are provided with opportunities to exercise their curiosity and develop their intellect free from the chilling effects of surveillance by educators, peers, parents, or commercial interests. As students begin to participate more fully in the online world, they must develop an appreciation for their own privacy and a corresponding respect for the privacy of others.

Clear Privacy Policies

It is important for libraries to develop privacy policies for student use of library resources that are adopted by both the library and the school's policy-making body. Students should be notified about library privacy policies when borrowing materials or accessing resources for the first time and as appropriate when there is a change in services, policies, or access. Library privacy policies should be made easily available and understandable to students in an age-appropriate manner. Safeguarding user privacy requires that staff keep all in-library use and reference questions confidential and assure that there is no monitoring by staff or peers of what students are reading, viewing, or researching while in the library.

Audit

School librarians should conduct privacy audits to determine the current threats to student privacy and what protections are already in place. The audit should cover the library management system; computer and network use in the library; eBooks and other online content; interactive Web tools; social media; and other technologies such as scanners/photocopiers and surveillance cameras. The results of the audit can be used to help create or revise privacy policies.

Collection and Retention of User Data

Libraries should limit the amount of personal information collected about students. Libraries should collect the minimum amount of personal information required to provide a service or meet a specific operational

need. Libraries should not build services or resources using sensitive personally identifiable information that, if leaked or accessed by an unauthorized party, could prove detrimental to the user's privacy.

Personally identifiable information should not be retained in perpetuity. The library should establish record retention policies specifying how long to retain different types of data and specifying methods for securely destroying data that is no longer needed. Retention policies should also cover archival copies and backups.

Encryption

The use of data encryption helps enhance privacy protection. All online transactions between client applications (staff desktop clients, web browsers, mobile apps, etc.) and server applications should be encrypted. Client applications that do not support encryption (such as staff desktop clients) should employ virtual private network (VPN) technologies. In addition, any personally identifiable information and student data housed by the library or school off-site (cloud-based infrastructure, tape backups, etc.) should use encrypted storage.

Data Sharing

Library privacy policies should define when school library records can be shared (and under what conditions) with parents or guardians, school staff and teachers, and third-parties such as online service providers.

Federal laws such as FERPA and COPPA as well as state laws concerning the confidentiality of library and student records may impact if and how data is shared. Because of the broad leeway FERPA gives schools in using student data for internal educational purposes, librarians need to clearly distinguish among library records, educational records, and administrative records in order to provide explicit privacy rights in accordance with professional ethical obligations.

Agreements between school libraries and online service providers should address appropriate restrictions on the use, aggregation, retention, and dissemination of students' personally identifiable information. Agreements between libraries and service providers should also specify that libraries retain ownership of all data and that the service providers agree to observe the library's privacy policies, data retention policy, and security policies. In the event of a data breach, users whose data was compromised should be informed promptly (in the case of minors, the parents or guardians should be informed).

Many service providers have signed the Student Privacy Pledge (studentprivacypledge.org/) which indicates a commitment to work in an ongoing fashion to meet and exceed all federal requirements to protect student data. Librarians should make participation in the Student Privacy Pledge a criterion when making purchasing decisions.

In addition, many states are passing legislation that restricts the collection and use of students' data by service providers (e.g. California's Student Online Personal Information Protection Act – SOPIPA). Librarians should only contract with service providers that comply with applicable state laws.

Educational Technology Systems

Primary and secondary schools are adopting learning management systems and other technologies that enable educators to monitor student reading habits (e.g. did the student access/read the assigned eBook or online text?) As a result, school districts are co-opting librarians into surveillance regimes by adopting these types of technologies. Librarians need to advocate for protecting student library use in an age of ubiquitous data logging and surveillance technologies, including learning management systems.

Digital Literacy & Advocacy
School librarians have a responsibility to teach students about their privacy rights, practices they can use to protect themselves, ethical behavior online, and respect for the privacy of others. In addition to educating students, school librarians should become advocates for protecting student privacy and intellectual freedom in the larger school environment. Often school librarians are focused only on user privacy within the library to the detriment of larger privacy issues in their school and district context. Because of their professional training and ethical commitment, librarians are well-equipped to be privacy advocates outside of the school library.

Additional Resources
Privacy Technical Assistance Center: ptac.ed.gov/
U.S. Department of Education
Privacy Toolkit: www.ala.org/advocacy/privacy/toolkit
ALA Intellectual Freedom Committee
Spying on Students: School-Issued Devices and Student Privacy: www.eff.org/issues/student-privacy
Electronic Frontier Foundation
Student Data Principles: studentdataprinciples.org/the-principles
Data Quality Campaign and the Consortium for School Networking
Student Privacy Bill of Rights: epic.org/privacy/student/bill-of-rights.html
Electronic Privacy Information Center
Student Privacy Pledge: studentprivacypledge.org/
Future of Privacy Forum (FPF) and The Software & Information Industry Association (SIIA)
Students' and Minors' Privacy Resources: chooseprivacyweek.org/students-and-minors-privacy/
Choose Privacy Week, American Library Association
Family Educational Rights and Privacy Act (FERPA): bit.ly/2kw9CCn
U.S. Department of Education
Complying with COPPA: Frequently Asked Questions: bit.ly/1H6xVOU
Federal Trade Commission
CA Student Online Personal Information Protection Act (SOPIPA): bit.ly/1wZHjfc

Approved April 2, 2016 by the Intellectual Freedom Committee of the American Library Association

ALA Library Privacy Checklist for Students in K – 12 Schools

This checklist is intended to help libraries of all capacities take practical steps to implement the principles that are laid out in the Library Privacy Guidelines for Students in K-12 Schools.

Priority 1 are actions that hopefully all libraries can take to improve privacy practices. Priority 2 and Priority 3 actions may be more difficult for libraries to implement depending on their technical expertise, available resources, and organizational structure.

Priority 1 Actions

1. Create internal library procedures to protect student privacy based on:

    a. school policies related to privacy and confidentiality of student data, especially student circulation records and the use of library resources in all formats.
    b. federal laws such as the Family Educational Rights and Privacy Act (FERPA), Children's Online Privacy Protection Act (COPPA), and state privacy laws regarding library records.
    c. ALA and AASL policy statements, online tool kits and Q & A's, guidelines, and other resources provided by national and state library associations.

2. Collect the minimum amount of information necessary about students to conduct library business.
3. Configure circulation software to delete students' borrowing history and retain only necessary records.
4. Ensure any paper records with sensitive information are stored in a secure area and shredded when no longer needed.
5. Train library staff and volunteers to respect students' privacy and the confidentiality of their library records.

Priority 2 Actions

1. Educate administrators, faculty, and support staff about students' library privacy and the confidentiality of student data using a variety of communication methods.

    a. Initiate conversations with the principal, teachers, students, and parents about the need for an official library privacy policy.

2. Add privacy-related resources to the library collection including items related to personal privacy, minors' privacy rights, and privacy as a national and international issue.

    a. Consider creating a privacy information section on the school library web page or a privacy-themed pathfinder (e.g., LibGuide) with privacy resources.

3. Integrate online privacy into library instruction and programming. For example:

    a. Introduce students to online privacy information such as secure passwords and web tracking during library orientations and other brief presentations.
    b. Celebrate Choose Privacy Week and other privacy-related observances (Data Privacy Day, Teen Tech Week, etc.) with the school community.
    c. Create privacy-related displays and set up videos in the library to educate parents during parent-teacher conferences and other evening school and community events
    d. Offer presentations to parents about students' privacy online and other topics of interest to families.

4. Advocate within the school or district for protecting students' privacy rights in learning management systems or other technologies that enable educators to monitor student reading and research

habits. Assessment should not include monitoring how students use specific library materials and online resources as part of free inquiry and research.
5. Volunteer to serve on the school's data governance committee. If one does not exist, advocate for its creation.

Priority 3 Actions

1. Work with other stakeholders in the school or district to create an official library privacy policy in regards to student circulation records and the use of library resources.

    a. The privacy policy should be approved by the school's governing body (e.g. school board, school committee, etc.)
    b. Post the policy in the library and on the library's section of the school website.
    c. Promote the library's privacy policy within the school community.

2. Work through school lines of authority to write or adapt a K-12 privacy curriculum and have it formally approved and taught. Collaboratively teach privacy units with teachers using the iKEEPSAFE and/or other privacy curricula.
3. Work with school officials to incorporate privacy protections into RFP's and resulting contracts. Discuss privacy concerns with digital resource and technology vendors, especially in regards to the school's/library's contracts with these vendors.
4. Ensure that all online transactions between client applications and server applications are encrypted.
5. Ensure that storage of personally identifiable student information is housed using encrypted storage.

Resources available online at http://www.ala.org/advocacy/privacy/checklists/students

Approved January 21, 2017 by the Intellectual Freedom Committee

Kent School District Library Media Program FERPA Guidelines

STUDENT LIBRARY CIRCULATION RECORDS ARE CONSIDERED CONFIDENTIAL RECORDS, UNDER THE FAMILY EDUCATIONAL RIGHTS & PRIVACY ACT (FERPA, FEDERAL LAW) AND WASHINGTON STATE LAW RCW 42.56.230: PERSONAL INFORMATION.

- Refrain from posting student library use information publicly.
- Refrain from sharing student information aloud in the presence of other students or non-involved staff.
- Overdue notices will be kept confidential and shared with only those necessary to assist the student with materials recovery (i.e. parent, guardian, teacher, and/or school cashier)
- Circulation of library materials will only be completed by library staff or KSD substitutes (who have received library privacy orientation).

CIRCULATION AND LIBRARY RECORDS CONTAINING STUDENT INFORMATION MUST BE KEPT CONFIDENTIAL AND SHREDDED.

THE SCHOOL LIBRARY WILL SUPPORT STUDENTS' INTELLECTUAL FREEDOM TO SELECT ANY MATERIAL OF THEIR CHOOSING.

- Students are welcome and encouraged to explore a variety of topics and genres, select books based on personal interest, and not only be restricted to checking out books at their reading level (i.e. AR, IRLA, etc.).
- A parent/guardian has the right to guide their child's use of the library and its resources and services.
- If a parent/guardian and their child determine that a library resource does not "fit" their child, it may be exchanged freely.
- Parents and guardians who do not want their children to have access to specific library materials should so advise their children.

School Library Privacy Checklist by Helen Adams

I have…	Met	Not Yet	Next Steps
✓ Educated myself about state and federal laws affecting minors' privacy in schools and libraries and reviewed American Library Association policy statements related to privacy and personally identifiable information (PII) about patrons.			
✓ Analyzed my state's library records law and understand how it applies to student library records.			
✓ Inquired how the Family Educational Rights and Privacy Act (FERPA) applies to school library records in my district.			
✓ Developed best practices operational privacy guidelines as a first step toward creating a school library privacy policy OR ✓ With other stakeholders developed a privacy policy that includes: description of PII collected, who may access library patron records, the circumstances under which minors' records may be released legally, FERPA guidelines, state library record law protections where applicable, and guidance for the extension of the maximum privacy protections possible. The draft			

was reviewed by the school district's legal counsel, and administration sought formal approval of the policy by the school board or institution's governing body.			
✓ Posted the library's privacy policy for patrons to read.			
✓ Created library procedures granting the maximum privacy possible to students regardless of age.			
✓ Protected circulation records with passwords and provide different levels of access for student assistants, adult volunteers, and library staff.			
✓ Configured automation software to delete students' circulation history.			
✓ Created a records retention policy that protects students' privacy by retaining library user records for the shortest period possible and destroyed records when they are no longer needed.			
✓ Retained as few student library records as possible; and purged library records identifying individual students' use of resources and services on a regular basis.			
✓ Trained library staff, volunteers, and student assistants about the confidentiality of all library records, instructing them not to examine circulation records of others.			
✓ Proactively educated administrators and teachers about student privacy and the confidentiality of library records.			
✓ Taught students to respect the confidentiality of library records – their own and those of others.			
✓ Informed students of overdue materials in a manner that respects their privacy.			
✓ Protected students' interlibrary loan and reserve requests from the scrutiny of non-library staff.			
✓ Modeled best practice by making sure that conversations with students about materials being checked out or used in the school library are confidential.			

✓ Guarded information gained through student use of resources and services by not divulging it indiscriminately to faculty, administrators, or others.			
✓ Refrained from affixing labels denoting a book's reading level or leveling a collection to avoid having students learn the reading levels of their peers.			
✓ Advocated for incorporating privacy into the district's acceptable use policy (AUP).			
✓ Included information about protecting one's privacy online as part of instruction on Internet safety.			
✓ Encouraged students to realize that citizens have privacy rights under the 4th and 5th Amendments, state, and federal laws.			
✓ Celebrated Choose Privacy Week (May) and Data Privacy Day (February) to raise awareness about privacy.			
✓ Reached out to parents by communicating library policy as it relates to student privacy and providing information about protecting minors' privacy online.			
✓ Demonstrated personal judgment when violating a student's privacy by speaking to a counselor or principal out of concern for a student's welfare or the safety of others.			
✓ Counseled that surveillance camera(s) not be aimed at the circulation desk or be intrusive in recording actions of persons using the school library.			
✓ Discussed privacy concerns with vendors of any technology currently owned or under consideration for purchase and requested that they include privacy protections in future software changes.			
✓ Prior to purchase, discussed with e-book lending and digital content vendors their collection of users' PII; tracking of digital content use; aggregation, anonymization, retention, and sharing of patron data; and security measures to ensure the protection of library patrons' privacy.			

✓ Collaborated with technology staff and faculty to evaluate apps, considering whether they collect PII, share data with third parties, and are compliant with FERPA.			

The checklist was developed by Helen R. Adams and originally published in *School Library Media Activities Monthly* vol. XXV, No. 7 (March 2009). It was revised in July 2012 and August 2015 to reflect new information.

Minors and Online Activity: An Interpretation of the Library Bill of Rights

The online environment offers opportunities for accessing, creating, and sharing information. The rights of minors to retrieve, create, and interact with information posted on the internet in schools and libraries are extensions of their First Amendment rights.

Schools and libraries should ensure that they offer opportunities for students to use social media and other online applications constructively in their academic and recreational pursuits. Students can enhance their social, interpersonal, and academic skills with the use of online applications. Some examples include:

- creating documents and sharing them online;
- uploading pictures, videos, and visual material;
- engaging in interactive games;
- classifying content and organizing information; and
- participating in online communities.

Online tools may help children and young adults learn about and organize social, civic, recreational, and academic activities. Many sites invite users to establish online identities, join networks, share personal information, and create web content. Library workers curate age-appropriate resources for academic and personal pursuits and teach children and young adults how to be safe online. Parents and guardians play a critical role in preparing their children for participation in online activity by communicating their values and guiding their children's use of the internet. Parents and guardians are only responsible for what their own children access online.

The use of social media and online resources poses two compelling intellectual freedom issues for minors: the right to free expression and the right to privacy.

Filters are often used in libraries and educational institutions to restrict access to online content, often limiting access to information and social media platforms beyond that required by the Children's Internet Protection Act and similar state laws. These restrictions deny minors' rights to free expression online.

Protection of minors' privacy rights online is also paramount. In addition to concerns about the vulnerability of young people who post personally identifiable information online, other threats to minors' privacy cause libraries and educational institutions to restrict and monitor minors' online activities. Perceived safety threats, such as cyberbullying, also lead to restrictive policies. These actions not only deny minors' right to free expression but may also deny their right to privacy.

Prohibiting minors from using social media or participating in online communities prevents youth from engaging in opportunities to learn and develop skills needed for responsible speech online, civil engagement, and personal privacy protection. Instead, libraries and library workers should educate youth about online activities that are appropriate for their maturity level without blocking access for others. Furthermore, library workers should advocate for implementing privacy-protecting policies and technology in libraries and educational institutions that both empower youth to take personal responsibility for their online privacy and prevent the collection and use of information about minors and their online activities for marketing and for-profit activities.

The First Amendment applies to all forms of speech created by minors and posted online. Restricting access to social media in schools and libraries limits young people's right to free expression and violates the tenets of the *Library Bill of Rights.* Instances of inappropriate use of social media and online applications should be addressed as individual behavior issues, not as justification for restricting or banning access to such tools. While other safety threats exist beyond schools' and libraries' physical space, these threats should not be a reason for limiting access for minors. Library workers, educators, and administrators have a responsibility to educate themselves about safety threats while continuing to advocate for the intellectual freedom of minors.

As defenders of intellectual freedom and the First Amendment, libraries have a responsibility to offer unrestricted access to online activity in accordance with local, state, and federal laws and to advocate for greater access where it is abridged. Of equal importance is the responsibility to advocate for minors' right to free expression and privacy online while using libraries of all types. In addition, library workers and educators should help young people learn digital citizenship skills that will prepare them to be responsible, effective members of a global society.

Adopted July 15, 2009, by the ALA Council; amended on July 1, 2014. Revisions proposed for ALA Annual Conference 2019.

Privacy: An Interpretation of the Library Bill of Rights

All people, regardless of origin, age, background, or views, possess a right to privacy and confidentiality in their library use.[1] When users recognize or fear that their privacy or confidentiality is compromised, true freedom of inquiry no longer exists.

Privacy is essential to the exercise of free speech, free thought, and free association. Federal and state courts have established a First Amendment right to receive information in a publicly funded library.[2] Further, the courts have upheld the right to privacy based on the U.S. Constitution. Many states provide guarantees of privacy in their constitutions and statute law.[3] Numerous decisions in U.S. case law have defined and extended rights to privacy to all.[4]

The right to privacy includes the right to open inquiry without having the subject of one's interest examined or scrutinized by others, in person or online. Confidentiality exists when a library is in possession of personally identifiable information about its users and keeps that information private on their behalf.[5] Article III of the ALA *Code of Ethics* states that confidentiality extends to "...information sought or received and resources consulted, borrowed, acquired or transmitted," including, but not limited to reference questions and interviews, circulation records, digital transactions and queries, as well as records regarding the use of library materials, services, programs, or facilities.

Protecting user privacy and confidentiality has long been an integral part of the mission of libraries. The ALA has affirmed a right to privacy since 1939.[6] Existing ALA policies affirm that confidentiality is crucial to freedom of inquiry. Rights to privacy and confidentiality are explicit in Article VII of the *Library Bill of Rights* and implicit in its guarantee of free access to library resources for all users.

Rights of Library Users

Lack of privacy and confidentiality has a chilling effect on users' selection, access to, and use of library resources. All users have a right to be free from any unreasonable intrusion into or surveillance of their

[1] Article VII, *Library Bill of Rights*

[2] Court opinions establishing a right to receive information in a public library include *Board of Education v. Pico*, 457 U.S. 853 (1982); *Kreimer v. Bureau of Police for the Town of Morristown*, 958 F.2d 1242 (3d Cir. 1992); and *Reno v. American Civil Liberties Union*, 117 S.Ct. 2329, 138 L.Ed.2d 874 (1997).

[3] Ten state constitutions guarantee a right of privacy or bar unreasonable intrusions into citizens' privacy. Forty-eight states protect the confidentiality of library users' records by law, and the attorneys general in the remaining two states have issued opinions recognizing the privacy of users' library records. See: State Privacy Laws Regarding Library Records.

[4] Cases recognizing a right to privacy include: *NAACP v. Alabama*, 357 U.S. 449 (1958); *Griswold v. Connecticut*, 381 U.S. 479 (1965); *Lamont v. Postmaster General*, 381 U.S. 301 (1965); *Katz v. United States*, 389 U.S. 347 (1967); and *Stanley v. Georgia*, 394 U.S. 557 (1969).

[5] The phrase "personally identifiable information" was adopted by the ALA in 1991. See the "ALA Policy Concerning Confidentiality of Personally Identifiable Information about Library Users."

[6] Article Eleven of the Code of Ethics for Librarians (1939) asserted that "It is the librarian's obligation to treat as confidential any private information obtained through contact with library patrons." See: Code of Ethics for Librarians (1939). Article Three of the 1995 ALA Code of Ethics states: "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."

lawful library use. ALA and its members recognize that children and youth have the same rights to privacy as adults. Library users expect, and in many places have, a legal right to have their personally identifiable information and library use data protected and kept private and confidential by anyone with access to that information. Libraries should never enact policies or practices that abridge users' right to privacy regardless of their age, housing status, immigration status, involvement with the criminal justice system, religious affiliation, ethnicity, sexual orientation, gender identity, or other forms of identity or status unless explicitly required by law. Even then, libraries should consult with legal counsel before abridging any users' right to privacy.

Libraries have a responsibility to inform users about policies and practices governing the collection, security, and retention of personally identifiable information and library use data. Additionally, users should have the choice to opt-in to any data collection that is not essential to library operations and the opportunity to opt-out again at any future time. All non-essential data collection should be turned off by default. In all areas of librarianship, best practice leaves users in control of as many choices as possible regarding their privacy. This includes decisions about the selection of, access to, and use of information. Information provided about users' choices should be prominently displayed, accessible, and understandable for a general audience.

Responsibilities in Libraries

The library profession has a long-standing ethic of facilitating, not monitoring, access to information. Libraries implement this commitment through the adoption of and adherence to library privacy policies that are consistent with applicable federal, state, local, and where appropriate, international law. It is essential that libraries maintain an updated, publicly available privacy policy that states what data is being collected, who it is shared with, and how long it is kept. Everyone who provides governance, administration, or service in libraries, including volunteers, has a responsibility to maintain an environment respectful and protective of the privacy of all users. It is the library's responsibility to provide ongoing privacy education and training to library workers, governing bodies, and users in order to fulfill this responsibility.

The *National Information Standards Organization (NISO) Consensus Principles on Users' Digital Privacy in Library, Publisher, and Software-Provider Systems* recognizes that

> [t]he 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.[7]

Libraries should not monitor, track, or profile an individual's library use beyond operational needs. Data collected for analytical use should be limited to anonymous or aggregated data and not tied to individuals' personal data. Emerging biometric technologies, such as facial recognition, are inconsistent with the mission of facilitating access to library resources free from any unreasonable intrusion or surveillance.

Regardless of the technology used, everyone who collects or accesses personally identifiable information in any format has a legal and ethical obligation to protect confidentiality. Library security practices to safeguard personal information should be up to date and in compliance with state and national standards. Adherence

[7] Principle 4, "Data Collection and Use," NISO Consensus Principles on Users' Digital Privacy in Library, Publisher, and Software-Provider Systems (NISO Privacy Principles) (2015)

to *NISO Consensus Principles on Users' Digital Privacy in Library, Publisher, and Software-Provider Systems* requires that these practices 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.[8]

Libraries should follow purpose limitation, storage limitation, and data minimization principles[9] when making decisions about collecting and retaining library use data. In particular, libraries should collect and store only personally identifiable data required for specific purposes that are disclosed to the users.

Libraries should periodically review their data collection and retention policies to identify situations in which the reason for collecting user data may no longer apply. Libraries may need to comply with state, institutional, or other governmental record retention policy in addition to developing their own data management policies. In addition, libraries should regularly review and update procedures for collecting and maintaining user data to ensure compliance with current industry privacy and security standards.

Libraries should never share users' personally identifiable information with third parties or vendors that provide resources and library services, unless the library obtains explicit permission from the user or if required by law or existing contract. Libraries or their governing institutions should negotiate agreements with vendors that retain library ownership of user data and permit independent auditing of vendor data collection, retention, and access policies and practices. Such agreements should stipulate that user data, is confidential, and that it may not be used or shared except with the permission of the library. Any vendor that handles user information as part of a library's service should have a publicly available privacy policy that commits to compliance with the *NISO Consensus Principles*. As existing contracts approach expiration, libraries should renegotiate future contracts to include these privacy safeguards.

Law enforcement agencies and officers may request library records and data that they believe contain information that would be helpful to the investigation of criminal activity. Libraries should have a procedure in place for handling law enforcement requests. Libraries should make such records available only in response to properly executed court orders or legal process. These court orders are issued following a showing of good cause based on specific facts by a court of competent jurisdiction.

The American Library Association affirms that rights of privacy are necessary for intellectual freedom and are fundamental to the ethical practice of librarianship. The rapid pace of information collection and changes in technology means that users' personally identifiable information and library use data are at increased risk of exposure. The use of new technologies in libraries that rely on the collection, use, sharing, monitoring and/or tracking of user data may come into direct conflict with the Library Bill of Rights and librarians' ethical

---

[8] *NISO Consensus Principles on Users' Digital Privacy in Library, Publisher, and Software-Provider Systems* (NISO Privacy Principles) (2015)

[9] These principles, drawn from the European Union General Data Protection Regulation (GDPR) (2018) and reflected in other fair privacy practice principles such as the *NISO Privacy Principles* and the *Organisation for Economic Co-operation and Development (OECD) Privacy Guidelines*, provide sound guidelines for libraries to follow in their data privacy practices. Libraries in the United States are not generally subject to the GDPR but should consult with legal counsel to determine whether GDPR applies to their library.

responsibilities. Libraries should consider privacy in the design and delivery of all programs and services, paying careful attention to their own policies and procedures and that of any vendors with which they work. Privacy is the foundation upon which our libraries were built and the reason libraries are such a trusted part of every community.

Adopted June 19, 2002, by the ALA Council; amended July 1, 2014. Revisions proposed for ALA Annual Conference 2019.

Questions and Answers on Privacy and Confidentiality: Minors' Privacy Rights

Are privacy rights of minors the same as those of adults? What information about a minor's use of the library should be kept confidential and what may be released to parents?

The rights of minors vary from state to state, and the legal responsibilities and standing of library staff in regard to minor users differ substantially in school, academic, and public libraries. Generally, a minor's right to keep his or her library records private will be governed by a state's library confidentiality statute; however, in public educational institutions, the Family Educational Rights and Privacy Act (FERPA) also determines the confidentiality and release of minors' library records. Libraries may wish to consult the legal counsel of their governing authorities to ensure that the library's policy and practice are in accord with applicable law.

In public libraries, parental responsibility is key to a minor's use of the library. Notifying parents about the library's privacy and confidentiality policies should be a part of the process of issuing library cards to minors. In some public libraries, the privacy rights of minors may differ slightly from those of adults, often in proportion to the age of the minor. The legitimate concerns for the safety of children in a public place can be addressed without unnecessary invasion of minors' privacy while using the library.

In public and school libraries, parents are responsible not only for the choices their minor children make concerning the selection of materials and the use of library facilities and resources, but also for communicating with their children about those choices. Library workers should not breach a child's confidentiality by giving out information readily available to the parent from the child directly. Libraries should take great care to limit the extenuating circumstances in which they will release such information.

Article VII of the *Library Bill of Rights* states "All 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." Article III of the *ALA Code of Ethics* directs library workers "to protect each library user's right to privacy and confidentiality." *Privacy: An Interpretation of the Library Bill of Rights* states: "All users have a right to be free from any unreasonable intrusion into or surveillance of their lawful library use. ALA and its members recognize that children and youth have the same rights to privacy as adults."

In all libraries, the rights of minors to privacy regarding their choice of library materials should be respected and protected. *Minors and Online Activity: An Interpretation of the Library Bill of Rights* asserts minors' right to seek, create, share, and interact with information on the Internet as extensions of their First Amendment rights. The statement also acknowledges that use of social media and web tools require the balancing of two intellectual freedom priorities — the preservation of minors' privacy and the right of free speech.

How does the Family Educational Rights and Privacy Act (FERPA) affect minors' library records in K-12 schools? Do state library records laws affect students' records?

"The Federal Educational Rights and Privacy Act," 20 U.S.C. § 1232g, (FERPA) controls disclosure of a student's educational records and information in both K-12 schools and post-secondary libraries. It requires educational institutions to adopt policies that permit parents of minor children to inspect and correct their educational records. It also prohibits disclosure of a student's records without the parents' written permission.

The Family Policy Compliance Office (FPCO), a part of the U.S. Department of Education, is the federal office charged with overseeing and enforcing FERPA. According to FPCO, any record maintained by an educational institution directly related to a student, in any format, that allows the student to be identified from the information contained in it, is considered an "educational record." FPCO staff have issued guidance stating that library circulation records and similar records maintained by a school library are "educational records" under FERPA.

Although FERPA generally requires institutions to protect the privacy of educational records, it contains many exceptions that allow disclosure of a student's educational records without a parent's or student's consent or permission. For example, FERPA permits educational institutions to release information contained in a student's records to any school official who has a "legitimate educational interest" in the records; to appropriate public officials in health and safety emergencies; and to courts and law enforcement agencies in response to a judicial order or lawfully issued subpoena. FERPA also permits educational institutions to disclose information about international students to the Department of Homeland Security and the Immigration and Customs Enforcement Bureau.

FERPA thus permits disclosure when state library confidentiality statutes and professional ethics would otherwise prohibit the disclosure of library records. FERPA, however, does not require the institution to disclose records under these circumstances, nor does FERPA require institutions to create or maintain particular records.

State library confidentiality laws may apply to K-12 libraries as well as public libraries and may impose additional responsibilities to protect students' library records that go beyond FERPA's requirements/permissions. Therefore, school libraries should craft policies that extend additional privacy protection to students' library records and, where applicable, incorporate state law protections for students' library records. The best protection lies in collecting the least amount of information and expunging it as quickly as possible.

How can the confidentiality of minors' library records be protected in school libraries?

The Library Privacy Guidelines for K-12 Students lay out both the challenges to and opportunities for protecting minors' privacy in public elementary, middle, and high schools. School libraries are often no longer independent entities and are frequently integrated into the district's administrative and technology infrastructure. As a result, it becomes more difficult for school librarians to act autonomously to implement privacy policies and practices when library resource management systems, digital resources, and other applications are tied into the districtwide infrastructure. It is now common for parents to be able to view the digital library records of their children in real time through the district's educational technology portal. In many districts, parents receive regular reports of the websites their children visit. These uses of technology seriously undermine students' privacy in school libraries.

31.What can school librarians do to protect their students' privacy?

It is critical that every school library have a privacy policy, approved by its governing body, outlining how students' library records are protected, and under what circumstances they may be released and to whom. The policy should refer to Article VII of the Library Bill of Rights, Article III of the ALA Code of Ethics, and other policy statements related to protecting minors' privacy rights in libraries. The privacy policy should reference and incorporate the state library confidentiality law, if applicable, and also include FERPA

guidelines. Without strong policies, school librarians will be left uncertain about the legal course of action and in a weaker position to respond to requests for release of library records.

After the privacy policy has been approved by the school's governing body, it should be disseminated to school staff, students, and parents. Minors' privacy and the confidentiality of their records will be better protected when school employees and the community understand the laws involved.

In addition to an official privacy policy, school libraries should also have a records retention policy detailing the types of records maintained, the length of retention, and a schedule for their expungement. Minors' records are best protected when minimal library records are maintained for the shortest period possible.

Beyond strong policies, school librarians can protect students' privacy through best practices such as by:

- Training library staff, volunteers, and student assistants about the legal and ethical nature of privacy in the library and the confidentiality of all library records.
- Educating teachers and administrators about student privacy and the confidentiality of library records.
- Teaching students to protect their personal privacy and respecting the privacy of others.
- Observing Choose Privacy Week during May 1-7 annually.
- Reaching out to parents to communicate library policies related to privacy.
- Collaborating with IT staff to evaluate technology-related hardware, software, filtering programs, and apps to ensure student privacy is protected.
- Discussing privacy concerns with vendors of current resources or those under consideration for purchase.

Additional Resources:

- Choose Privacy Every Day -Resources/Minors & Students
- ALA Privacy Guidelines for Students in K-12 Schools
- ALA Privacy Checklist for Students in K-12 Schools

ALA Library Privacy Guidelines

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 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.

---

[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

Approved June 29, 2015 by the Intellectual Freedom Committee of the American Library Association

Library Privacy Guidelines for Library Management Systems

Introduction
Library management systems (LMS), also known as integrated library systems, are used by libraries to inventory collections and manage user records. The LMS stores personal information collected from patrons for a variety of reasons and maintains records of what items patrons borrow, the holds they place, and fines or fees they may incur. In addition, the LMS may share data with or provides services to other systems employed by the library, for example to provide authentication for online resources.

Libraries must work to ensure that their procedures and practices for managing the LMS reflect library ethics, policies, and legal obligations concerning user privacy and confidentiality. Agreements between libraries and vendors should specify that libraries retain ownership of all data; that the vendor agrees to observe the library's privacy, data retention, and security policies; and that the vendor agrees to bind any third parties it uses in delivering services to these policies as well.

These guidelines are issued by ALA to provide libraries using LMS with information about appropriate data management and security practices in respect to library patrons' personally identifiable information and

data about their reading habits and use of library resources.

Why Privacy Is Important
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. Librarians and libraries may also have a legal obligation to protect library users' personally identifiable information and data from unauthorized disclosure and use.

Clear Privacy Policies
Users should be notified about library privacy policies when registering for a library card or borrowing materials for the first time. Library privacy policies should be made easily available and understandable to users in an accessible format. Safeguarding user privacy requires that individuals know what personally identifiable information is gathered about them, how long it is stored, who has access to it and under what conditions, and how it is used. A proactive process should be created to notify ongoing users of any changes to the library's privacy policies.

User Consent
The library should give users of the LMS options as to how much personally identifiable information is collected from them and how it may be used. Users should have a choice about whether to opt-in to features and services that require the collection of personal information. Users should also have the ability to opt-out if they later change their minds and have the data collected during the opt-in phase be destroyed when possible. For example, if the LMS offers the ability to save the checkout history, this should be an opt-in feature not turned on as a default.

Access to Personal Data
Users should have the right to access their own personal information and evaluate its accuracy. Verifying accuracy helps ensure that library services that rely on personally identifiable information can function properly. Guidance on how the user can access their personal data held in the LMS should be clear and easy to find.

Access to personal information should be restricted to the user or appropriate library staff and conform to the applicable state laws addressing the confidentiality of library records as well as other applicable local, state, and federal law. In addition, state and federal laws may give parents, guardians, and educators access to the library records of minors (see *Library Privacy Guidelines for Students in K-12 Schools* in the Additional Resources section below).

Collection & Retention of User Data
Libraries should limit the amount of personal information collected by the LMS about patrons. In general, the library should collect the minimum amount of personal information required to provide a service or meet a specific operational need. Library policies developed around the collection of personal information should also cover the use of any free-text note fields associated with the patron's record. Personally identifiable information should not be retained in perpetuity. The library 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.

Encryption
All online transactions between client applications (staff desktop clients, web browsers, mobile apps, etc.) and server applications should be encrypted using modern, up-to-date security protocols for SSL/HTTPS. Client applications that do not support encryption (such as staff desktop clients) should employ virtual private network (VPN) technologies. In addition, any personally identifiable information and user data housed by the library off-site (cloud-based infrastructure, tape backups, etc.) should use encrypted storage.

PINs & Passwords
User personal identification numbers (PINs) and passwords stored in the LMS should be encrypted so that only the user has access to them, i.e. library staff cannot view them. This encryption should use up-to-date best practices. Currently, this means that passwords should be salted and hashed with a SHA-2 hash function, but library personnel responsible for password security should stay current on best practices. In addition, the LMS should provide users

with the ability to set their PIN or password themselves without having to reveal it to library staff.

Notifications & Reports
User notifications for holds, overdue items, and fines should contain minimal personal information especially if sent through insecure communication (e.g. email, text message, postcards). Users could be encouraged to login to a secure account for more details. If the LMS provides the ability to include notification history as part of the patron record, this should be offered as an opt-in feature for patrons and not turned on by default.

Access to LMS reports that contain personally identifiable information should be restricted to appropriate library staff. Reports intended for wider distribution should be anonymized by removing or encrypting personally identifiable information. Libraries that combine patron information from the LMS with external demographic information for analytics should take measures to protect reader privacy. Aggregation and anonymization should be employed to help prevent the identification of reading habits and library usage with specific individuals. Because of the growing threat of reidentification techniques, access to anonymized data sets should still be restricted to appropriate users.

Data Sharing
It has become common practice for organizations to share data including personally identifiable information with third-parties. However, 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, although some state library confidentiality statutes permit sharing this data with parents or guardians of minors. In addition, ALA policy forbids sharing of library patron information with third parties without user consent or a court order.

Government Requests
The library should develop and implement procedures for dealing with government and law enforcement requests for library patrons' personally identifiable information and use data held within the LMS. The library 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 library should also inform users through its privacy policies about the legal conditions under which it might be required to release personally identifiable information.

The library could consider publishing a warrant canary notice to inform users that they have not been served with a secret government subpoena or national security letter. If a canary notice is not updated or it is removed, users can assume that a subpoena or national security letter has been served (see Canary Warrants Frequently Asked Questions in the Additional Resources section below).

Privacy Awareness
Library staff who have access to patron data in the LMS should receive training on the library's privacy policies and best practices for safeguarding patron privacy. Libraries 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. A library that suffers a violation in its privacy policies through inadvertent dissemination or data theft must notify the affected users about this urgent matter as soon as the library is aware of the data breach and describe what steps are being taken to remedy the situation or mitigate the possible damage.

Additional Resources
Canary Warrants Frequently Asked Questions
Electronic Frontier Foundation
Library Privacy Guidelines for Students in K-12 Schools, Intellectual Freedom Committee of the American Library Association
NISO Consensus Principles on User's Digital Privacy in Library, Publisher, and Software-Provider Systems, National Information Standards Organization
Privacy Toolkit, Intellectual Freedom Committee of the American Library Association

Approved June 24, 2016 by the Intellectual Freedom Committee of the American Library Association

Data Exchange Between Networked Devices and Services

Introduction
Machine-to-machine communications of data allow libraries to offer services such as self-checkout stations and patron account features in library catalogs. A

typical scenario might be an application installed on a library management system that allows a client application to access patron data and perform transactions or perform information searches on behalf of a patron. Examples of protocols and APIs supported by many library management systems include SIP2, NCIP, Z39.50, SRU and SRW, and other Web services (see Glossary of Terms at the end of this document). Libraries must work to ensure that their procedures and practices for managing programmatic data communications reflect library ethics, policies, and legal obligations concerning user privacy and confidentiality.

These guidelines are issued to provide libraries with information about appropriate data management and security practices in respect to library patrons' personally identifiable information and data about their reading habits and use of library resources.

Why Privacy Is Important

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. Librarians and libraries may also have a legal obligation to protect library users' personally identifiable information and data from unauthorized disclosure and use.

Encryption

The use of data encryption helps enhance privacy protection. Data communications between client applications and server applications that may include patron information should be encrypted. Client-server applications that do not support encryption (such as SIP2) should be deployed over transports that perform encryption, such as virtual private networks (VPNs) or TLS or SSH tunnels. If a particular service or protocol is available over either encrypted or unencrypted connections (e.g., as can be the case with NCIP), the library should mandate the use of the encrypted configuration option.

Access Control

Server applications that allow programmatic data communications should limit access to authorized client applications. The library should monitor server applications to insure no unauthorized client applications have access to patron information as a standard part of data security measures.

Minimum Disclosure

Server applications that allow programmatic data communications should supply only the minimum of patron information required to fulfill the specific purpose for which that information is being made available to an authorized client application. For example, if a client application needs to verify that a set of credentials correspond to those of a patron who has privileges at the library, that application may not need to be sent any contact or demographic information about that patron. The library should take advantage of available configuration options to enforce the principle of minimum disclosure.

The library should work with service and system providers to perform an audit which identifies what data is currently being transmitted, kept, and under what circumstances in order to ensure minimum disclosure in the future.

Retention of User Data

Server applications that provide programmatic data communications may create log files that contain patron information. The library should establish policies for how long to retain log files and methods for securely destroying data that is no longer needed. Retention policies should also cover archival copies and backups.

Standards Development

Librarians and library technologists who participate in the design of new standards or application profiles for machine-to-machine communication protocols should advocate for standards that follow these guidelines.

Glossary of Terms

API - application programming interface is a set of routine definitions, protocols, and tools for building software and applications.

Client - a piece of computer hardware or software that accesses a service made available by a server. The server is often (but not always) on another computer system, in which case the client accesses the service by way of a network.

NCIP - National Information Standards Organization Circulation Interchange Protocol is a protocol that is limited to the exchange of messages between and among computer-based applications to enable them to perform functions necessary to lend and borrow items, to provide controlled access to electronic resources, and to facilitate cooperative management of these functions.
SIP2 - Standard Interchange Protocol 2 is a proprietary standard for communication between library computer systems and self-service circulation terminals.
SRU - Search/Retrieve via URL is a standard search protocol for Internet search queries, utilizing Contextual Query Language (CQL), a standard query syntax for representing queries.
SRW - Search/Retrieve Web service is a web service for search and retrieval.
SSH tunnel - an encrypted tunnel created through an SSH protocol connection. Users may set up SSH tunnels to transfer unencrypted traffic over a network through an encrypted channel.

Approved June 24, 2016 by the Intellectual Freedom Committee of the American Library Association

Library Websites, OPACs, and Discovery Services

Introduction
Libraries publish information and provide services through websites, online public access catalogs (OPACs), and discovery services. The OPAC, often known simply as the library catalog, allows patrons to search the library's collections using a web-based user interface. A discovery service provides a single web-based user interface to search across multiple resources such as library catalogs, periodical databases, institutional repositories, and digital collections.

Library websites, OPACs, and discovery services may collect personal information about patrons for a variety of reasons including authentication, personalization, and user analytics. In addition, personal information is sometimes shared with third parties that provide content or other functionality for the website or service.

The hardware, applications, and data that comprise a website or service may be managed directly by the library; by a parent organization such as a local government, school, or consortium; by a vendor or service provider; or by some hybrid of shared responsibilities among multiple parties. Regardless of the management model, libraries must work to ensure that the websites, OPACs, and discovery services they offer reflect library ethics, policies, and legal obligations concerning user privacy and confidentiality.

These guidelines are issued to provide libraries with information about appropriate data management and security practices in respect to library patrons' personally identifiable information and data about their reading habits and use of library resources.

Why Privacy Is Important
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 responsibility, expressed in the ALA Code of Ethics, to preserve users' right to privacy. Librarians and libraries may also have a legal obligation to protect library users' personally identifiable information and data from unauthorized disclosure and use.

Clear Privacy Policies
Users should be notified about library privacy policies when using a library website, OPAC, or discovery service. Library privacy policies should be made easily available and understandable to users in an accessible format. Safeguarding user privacy requires that individuals know what personally identifiable information is gathered about them, how long it is stored, who has access to it and under what conditions, and how it is used. A proactive process should be created to notify ongoing users of any changes to the library's privacy policies.

Personalization & User Consent
The library should give users options as to how much information is collected from them and how it may be used. Users should have a choice about whether to opt-in to features and services that require the collection of personal information. Users should also have the ability to opt-out if they later change their minds and have the data collected during the opt-in phase be destroyed when possible. For example, if the

discovery service offers the ability to save their search history, this should be an opt-in feature not turned on as a default.

Access to Personal Data
Users should have the right to access their own personal information and evaluate its accuracy. Verifying accuracy helps ensure that library services that rely on personally identifiable information can function properly. Guidance on how the user can access their personal data should be clear and easy to find.

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

Encryption
All online transactions between client applications (web browsers, e-book readers, mobile apps, etc.) and server applications should be encrypted using modern, up-to-date security protocols for SSL/HTTPS. Communications between server applications and third-party service providers should be encrypted. User passwords should be stored using up-to-date best practices for encryption. In addition, any personally identifiable information and user data housed off site (cloud-based infrastructure, tape backups, etc.) should use encrypted storage.

Data Sharing
It has become common practice for organizations to share data, including personally identifiable information with third-parties, often unintentionally. Scripts and embedded content from a third-party that are placed on websites (sharing buttons, photo streams, videos, etc.) may allow that third party to track user behavior and share that data with other parties. However, 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 without user consent or a court order.

Libraries should carefully evaluate the impact on user privacy of all third-party scripts and embedded content that is included in their website, OPAC, or discovery service.

User Generated Content
Library websites, OPACs, and discovery services often allow patrons to create publicly shared content such as comments, ratings, recommendations, etc. The library will need to weigh the costs and benefits of requiring authentication (privacy implications if real identity is used) versus anonymous access (more difficult to prevent spam and other unacceptable use) in order to create shared content. In addition, tools that allow the creation of content may rely on third parties which may collect user data and share it with other parties.

Activity Data & Web Analytics
Libraries should limit the amount of personal information collected about users. Websites, OPACs, and discovery services collect and record data about user activity. Even for anonymous users (I.e. those that do not login to access personalization features) the activity data may include personally identifiable information. In general, the library should collect the minimum personal information required to provide a service or meet a specific operational need. Access to reports that contain personally identifiable information should be restricted to appropriate library staff. Reports and web analytics intended for wider distribution should be anonymized by removing or encrypting personally identifiable information. Careful consideration should be given before using a third party to collect web analytics (e.g. Google Analytics) since the terms of service often allow the third party to harvest user activity data for their own purposes.

User activity data with personally identifiable information should not be retained in perpetuity. The library should establish policies for how long to retain different types of data and methods for securely destroying data that is no longer needed. Retention policies should also cover archival copies and backups.

Privacy Awareness
Library staff who manage the library's websites and services should receive training on the library's privacy policies and best practices for safeguarding patron privacy. Library staff that negotiate contracts with vendors that provide websites and services should also receive privacy training.

Libraries 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. A library that suffers a violation in its privacy policies through inadvertent dissemination or data theft must notify the affected users about this urgent matter as soon as the library is aware of the data breach and describe what steps are being taken to remedy the situation or mitigate the possible damage.

Additional Resources

Let's Encrypt, Internet Security Research Group
NISO Consensus Principles on User's Digital Privacy in Library, Publisher, and Software-Provider Systems, National Information Standards Organization
Privacy: An Interpretation of the Library Bill of Rights, American Library Association
Privacy Toolkit, Intellectual Freedom Committee of the American Library Association

Approved June 24, 2016 by the Intellectual Freedom Committee of the American Library Association

Public Access Computers and Networks

Introduction

Libraries provide patrons with opportunities to use computers and other devices (e.g. laptops, tablets, e-book readers, etc.) to access online resources such as library catalogs, research databases, eBooks, other digital content, and the Internet. Patrons use library computers to create content including word processing documents, multimedia projects, email messages, and posts to social media and other websites. In addition, libraries often provide wired and wireless public networks that allow patrons to connect using a personal device.

Use of any computer or network may create records of users' activities that can jeopardize their privacy. In addition, libraries may collect personal information from users for a variety of reasons such as reserving a computer or checking out a device. Libraries must work to ensure that their procedures and practices for managing public access computers and devices reflect library ethics, policies, and legal obligations involving user privacy and confidentiality.

These guidelines are issued to provide libraries with information about appropriate data management and security practices with respect to library patrons' personally identifiable information and data about their use of public access computers and networks.

Why Privacy Is Important

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 responsibility, expressed in the ALA Code of Ethics, to preserve users' right to privacy. Librarians and libraries may also have a legal obligation to protect library users' personally identifiable information and data from unauthorized disclosure and use.

Clear Privacy Policies

Users should be notified about library privacy policies when accessing a computer or a public network in the library. The privacy policies should be made easily available and understandable to users. Safeguarding user privacy requires that individuals know what personally identifiable information is gathered about them, how long it is stored, who has access to it and under what conditions, and how it is used. A proactive process should be created to notify ongoing users of any changes to the library's privacy policies.

Access Control & Device Checkout

Libraries can use a variety of methods to manage access to computers and networks. These methods range from a clipboard with a sign-up sheet to sophisticated access control software that can include user authentication, reservations, time limits, and management of Internet content filters. The integrated library system may be used to checkout laptops and other devices. In addition, libraries may require users to authenticate in order to access the network when using their personal device.

Whatever methods are employed, libraries should develop appropriate policies and procedures to protect the privacy of patrons and their computer and network activity in the library. Transactional logs generated by access control software and network authentication should be anonymized or destroyed when no longer needed. Sign-up sheets should be redacted or

shredded. Checkout records should be purged or anonymized when the device is returned and any overdue fines paid.

Display Screens
Computer display screens are often easily visible to nearby people. Libraries should make privacy screens or recessed displays available to patrons who desire to use them while recognizing no screen will render a user's display completely invisible to other people. In addition, many people dislike privacy screens or recessed displays and therefore should not be forced to use them.

Browser Activity
Many websites track user behavior and share data with third parties via cookies and other technologies. The library should provide browsers and plugins that offer privacy protections when surfing the Web. In addition, browsers should be configured to clear all data (cache, history, cookies, passwords) upon exit.

Routine Maintenance
Public computers should be routinely maintained to ensure they are operating properly, and that the software on the computer designed to protect the user's privacy is activated and effective. A security audit of the computer could be routinely performed to attempt to locate deficiencies in the security of the computer. A physical inspection should also include the identification of unknown devices attached to the computer designed to steal personal information such as keyloggers.

Personal Data on Computer or Device
Use of any computer or device may create records of the user's activities that can jeopardize their privacy. Documents, emails, and other files that may contain private information could be left on the device. The library should use restoration software or other technological means to remove traces of individual use on public access computers and other devices provided by the library.

Malware
Malware can be a serious threat to personal privacy and security when using a computer. If the malware captures login information and passwords, the user's online accounts maybe compromised. Libraries should take appropriate steps to ensure that malware or other unauthorized software does not reside on the computer or device. These steps could include security protection (anti-malware, anti-spam, anti-virus programs) as well as restoration software to remove all software installed without authorization.

Computer Monitoring & Usage Tracking
Monitoring software can be installed to record activities or remotely view what a user is doing on a device. It is often used for technical support or for compliance with an organization's computer use policy. To protect users' privacy, libraries should avoid using monitoring software on public access computers or other devices provided by the library. If monitoring is employed, users should be informed of its purpose and scope in the library's privacy policies.
Many applications and operating systems are configured by default to automatically share activity data with the software publisher to identify errors, enhance usability, or provide personalization. When possible, the library should disable such usage tracking on public access computers or other devices provided by the library.

Approved June 24, 2016 by the Intellectual Freedom Committee of the American Library Association

Fair Information Practice Principles

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.[10]

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.

[10] 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 principles into their privacy policies.
See, also guidance at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-.pdf.

Notes

Contact

Office for Intellectual Freedom
American Library Association
50 East Huron Street
Chicago, Illinois 60611
www.ala.org/oif

Deborah Caldwell-Stone, Interim Director
dstone@ala.org
312-280-4224

Kristin Pekoll, Assistant Director
kpekoll@ala.org
312-280-4221

Eleanor Diaz, Program Officer
ediaz@ala.org
312-280-4225

Yumeka Brown, Program Officer
ybrown@ala.org
312-280-4226

Presenters

Helen Adams
hadams1@centurytel.net

Candice (Wing-yee) Mack
candic.YALSA@gmail.com

ALA American Library Association