American Library Association Guidelines for Developing a Library Privacy Policy

Prepared by the ALA Intellectual Freedom Committee, August 2003
http://www.ala.org/offices/oif/iftoolkits/toolkitsprivacy/libraryprivacy

Prepared by the ALA Intellectual Freedom Committee, August 2003

I. Introduction

Privacy is essential to the exercise of free speech, free thought, and free association. In libraries, the right to privacy is the right to open inquiry without having the subject of one's interest examined or scrutinized by others. Confidentiality exists when a library is in possession of personally identifiable information (PII) about users and keeps that information private on their behalf.

With technology changes, increased incidence of identity theft, and new laws, as well as increased law enforcement surveillance, librarians must act now to develop and/or revise their privacy policies and procedures in order to ensure that confidential information in all formats is protected from abuse. They must also protect their organizations from liability and public relations problems. When developing and revising policies, librarians need to ensure that they:

- Limit the degree to which personally identifiable information is monitored, collected, disclosed, and distributed.
- Avoid creating unnecessary records.
- 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.
- Avoid library practices and procedures that place personally identifiable information on public view.

A privacy policy communicates the library's commitment to protecting users' personally identifiable information. A well-defined privacy policy tells library users how their information is utilized and explains the circumstances under which personally identifiable information might be disclosed. When preparing a privacy policy, librarians need to consult an attorney in order to ensure that the library's statement harmonize with the many state and federal laws governing the collection and sharing of personally identifiable information.

Libraries need to post privacy policies publicly. Privacy: An Interpretation of the Library Bill of Rights states that, "Users have the right to be informed what policies and procedures govern the amount and retention of personally identifiable information, why that information is necessary for the library, and what the user can do to maintain his or her privacy."

PII: Personally Identifiable Information

One of the key concepts to understand when developing policies and procedures is that defined as: "Personally identifiable information" (PII). PII has become the generally accepted language; ALA began using this term in 1991 when it adopted the Policy Concerning Confidentiality of Personally Identifiable Information about Library Users. PII connects individuals to what they bought with their credit cards, what they checked out with their library cards, and what Web sites they visited where they picked up cookies. More than simple identification, PII can build up a picture of tastes and interests—a dossier of sorts, though crude and often inaccurate. While targeted advertising is the obvious use for PII, some people would use this information to assess their character, decide if they were a security risk, or embarrass them for opposing a particular position. Because of the chilling effect that such scrutiny can have on open inquiry and freedom of expression, libraries and bookstores have long resisted requests to release information that connects individual persons with specific books.

Privacy Policies and the Law

Library privacy and confidentiality policies must be in compliance with applicable federal, state, and local laws. The courts have upheld the right to privacy based on the Bill of Rights of the U.S. Constitution. Many states provide guarantees of privacy in their constitutions and statute law. Numerous decisions in case law have defined and extended rights to privacy.

Privacy Policies and ALA

A number of ALA policies and recommendations have been passed in recent years on privacy and confidentiality issues. But recognition of the importance of this issue dates back as far as the 1930's in ALA policy. 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." Article Three of the current Code (1995) 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."

Your Library's Policy Should Incorporate Standard Privacy Principles

In addition to ALA policies, there are many very good frameworks for establishing privacy policies. The privacy policy guidelines outlined here are based in part on what are known as the five "Fair Information Practice Principles." These five principles outline the rights of Notice, Choice, Access, Security, and Enforcement. Another widely accepted European legal framework establishing rights of data privacy and confidentiality calls for ensuring Collection limitation, Data quality, Purpose specification, Use limitation, Security safeguards, Openness, Individual participation, and Accountability. These frameworks provide the basis for recommendations from other consumer and privacy advocacy groups, whose checklists are well worth reviewing.

II. How to Draft a Library Privacy Policy (a Model Privacy Policy is attached as Appendix 1 to this document)

All types of libraries are urged to draft and/or revise privacy and confidentiality policies. This document offers guidance for public, academic, research, school, and special libraries, as well as library systems. Special considerations are raised in Section III for school and academic libraries and for public library services to minors because each are affected by laws and practices unique to those particular situations. Other considerations may also apply. When drafting a policy, library administrators should check with their parent institutions to ensure they are complying with appropriate norms and policies. Some elements of this guidance may not pertain to all libraries.

1. Notice & Openness

Policies should provide notice to users of their rights to privacy and confidentiality and of the policies of the library that govern these issues. Such notice should dictate the types of information gathered and the purposes for and limitations on its use. It is critical that library privacy policies be made widely available to users through multiple means. This is because safeguarding personal privacy requires that individuals know what personally identifiable information (PII) is gathered about them, where and how it is stored (and for how long), who has access to it and under what conditions, and how that PII is used.

Examples of User Notice Statements from Sample Library Privacy Policies:

Queens Borough Public Library http://m.queenslibrary.org/about-us/privacy

2. Choice & Consent

Choice means giving users options as to how any personal information collected from them may be used. Provision of many library services requires the collection and retention of personally identifiable information. Whether this is required (e.g. in order to circulate library material), automatic (e.g. as in some Web-based library services), or voluntary (e.g. when engaging in e-mail-based reference), this information should be retained only as long as is necessary to fulfill the function for which it was initially acquired. Two commonly used schemes for choice/consent are "opt-in," where the default is not to include the information and affirmative steps are required for inclusion, or "opt-out" where the default is to include the information and affirmative steps are required for exclusion.

Examples of Choice and Consent Statements from Sample Library Privacy Policies:

- Duke University Library http://library.duke.edu/about/privacy

3. Access by Users

Users have the right of access to their own personally identifiable information (PII). The right to this access should be mentioned in the privacy policy. Verifying the accuracy and status of PII helps ensure that library services that rely on personally identifiable information can function properly. The right of access covers all types of information gathered about a library user or about his or her use of the library, including mailing addresses, circulation records, computer use logs, etc. Access to personal information should be made available onsite or through online access with security parameters in effect to verify the existence of individual users.

Right to access should also address instances in which age may be a factor. The Children's Online Privacy Protection Act of 1998 (COPPA) provides for "a parent's ability to review, make changes to, or have deleted the child's personal information." For more on COPPA, see the section called "School Library Media Centers" below under Part III.

4. Data Integrity & Security

Data Integrity: The library needs to assure data integrity. Whenever personally identifiable information (PII) is collected, the library must take reasonable steps to ensure integrity, including using only reputable sources of data, providing consumer access to data, updating information regularly, destroying untimely data or converting it to anonymous form, and stripping PII from aggregated, summary data. It is the responsibility of library staff to destroy information in confidential or privacy-protected records in order to ensure unauthorized disclosure. Information that should be regularly purged or shredded includes PII on library resource use, material circulation history, security/surveillance tapes and use logs, both paper and electronic.

Shared Data: If patron records are supplied by or shared with a parent institution such as a college registrar or a library consortium, the library needs to adopt measures to ensure timely corrections and deletions of data. Likewise, when the library exchanges data with other departments such as bursars and tax collectors, vendors, or any other organizations, it must ensure that records are accurate and up to date. Libraries issuing passwords should avoid choosing passwords or PIN's that can reveal a user's identity, including social security numbers.

Security: Security involves both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data. Security measures should be integrated into the design, implementation and day-to-day practices of the library's entire operating environment as part of its continuing commitment to risk management. These measures are intended to prevent corruption of data, block unknown or unauthorized access to library systems and information, and provide reasonable protection of private information in a library's custody, even if stored offsite on servers or back up tapes.

Administrative Measures: The library needs to implement internal organizational measures that limit access to data while ensuring that those individuals with access do not utilize the data for unauthorized purposes. The library must also prevent unauthorized access through such technical security measures as including encryption in the transmission and storage of data; limits on access through use of passwords; and the storage of data on secure servers or computers that are inaccessible by modem or network connection. If libraries store PII on servers or back up tapes that are offsite, they must ensure that comparable measures to limit access to data are followed. Libraries should develop routine schedules for shredding PII collected on paper.

Electronic Tracking: Neither local nor external electronic systems used by the library should collect PII by logging or tracking e-mail, chat room use, Web browsing, cookies, middleware, or other usage. Nevertheless, users should be advised of the limits to library privacy protection when using remote sites. If the library enables cookies (small files sent to a browser by a Web site to enable customization of individual visits), it should alert users how to refuse, disable, or remove cookies from their hard drives. In addition, the library should not maintain cookies after users terminate their sessions nor share them with external third parties. Libraries should regularly remove cookies, Web history, cached files, or other computer and Internet use records and other software code that is placed on their networks. Those libraries that authenticate patrons for use of external databases by middleware systems and/or proxy servers should simply verify the attributes of valid users and not release PII.

Data Retention: It is the responsibility of library staff to destroy information in confidential or privacy-protected records in order to safeguard data from unauthorized disclosure. Information that should be regularly purged or shredded includes PII on library resource use, material circulation history, and security/surveillance tapes and logs. If this data is maintained off site, library administrators must ensure that appropriate data retention policies and procedures are employed. Libraries that use surveillance cameras should have written policies stating that the cameras are not to be used for any other purpose. If the cameras create any records, the library must recognize its responsibility to protect their confidentiality like any other library record. This is best accomplished by purging the records as soon as their purpose is served.

Encryption: Data encryption can be used to enhance privacy protection. Encrypted data requires others to use a pre-defined electronic "key" to decipher the contents of a message, file, or transaction. Libraries should negotiate with vendors to encourage the use of such technology in library systems (e.g., in the document delivery, saved searches, and e-mail features now offered by many OPAC vendors). Whenever possible, libraries should consider making encryption tools available to library users who are engaging in personalized online transactions or communications.

Selected Links:

- Cookie Central, "Frequently Asked Questions About Cookies" http://www.cookiecentral.com/faq/
- The Electronic Privacy Information Center, "Cookie Page" http://epic.org/privacy/internet/cookies/
- The Electronic Privacy Information Center, "International Data Retention Page" http://epic.org/privacy/intl/data_retention.html
- International Coalition of Library Consortia, Privacy Guidelines for Electronic Resources Vendors http://icolc.net/statement/privacy-guidelines-electronic-resources-vendors
- Internet2, The Shibboleth Project http://www.internet2.edu/products-services/trust-identity-middleware/shibboleth/
- Duke University Library http://library.duke.edu/about/privacy

5. Enforcement & Redress

Libraries that develop privacy policies need to establish and maintain an effective mechanism to enforce them. They should conduct regular privacy audits in order to ensure that all library programs and services are enforcing this privacy policy. Redress must be available for library users who feel their privacy and confidentiality rights are violated. Libraries should provide a means to investigate complaints and re-audit policy and procedures in cases of potential violation of library privacy and confidentiality. Library educational efforts should include informing users how to protect their own privacy and confidentiality, both in and outside of the library setting.

Libraries must ensure they have well-established procedures to enforce their policies by informing users about the legal conditions under which they might be required to release personally identifiable information (PII). Libraries should only consider a law enforcement request for any library record if it is issued by a court of competent jurisdiction that shows good cause and is in proper form. Only library administrators after conferring with legal counsel should be authorized to accept or comply with subpoenas, warrants, court orders or other investigatory documents directed to the library or pertaining to library property. All library staff, however, should be trained and required to contact a designated Library Privacy Officer or previously designated administrator immediately should a law enforcement officer appear and request the library comply with a request to release PII.

Libraries should develop and implement procedures for dealing with law enforcement requests before, during, and after a visit. Guidance on these matters can be found in the following ALA documents:

- Confidentiality and Coping with Law Enforcement Inquiries: Guidelines for the Library and its Staff, April 2002
- Suggested Procedures for Implementing Policy on Confidentiality of Library Records, 1988
- USA PATRIOT Act, May 2003:

III. Special Privacy Policy Considerations: Academic Libraries, School Libraries, and Public Library Services to Minors

Academic Libraries

The heart of the mission of academic institutions is the freedom to research unfamiliar and controversial topics. Academic libraries serve those needs well. Often, they offer their personal, professional, and educational information services to a wide variety of users. If academic libraries provide different levels of service or access to different categories of borrowers (e.g., faculty, graduate students, undergraduate students, or community members), they must ensure that their services and access are offered equitably within a borrower type. Such restrictions should not impede intellectual freedom.

Academic Libraries and Students: Students in academic institutions are adults and must be accorded the same privacy safeguards as adults in other types of libraries. The mere fact that students are enrolled in courses should not jeopardize their privacy rights. Thus, student circulation records for course-required and reserve reading should be protected from inquiry with the same rigor as their circulation records for personal reading. Librarians assisting in investigations of plagiarism should take care to protect the usage records of individual students. Librarians can assist faculty in the development of classroom instruction and procedures that meet educational goals without compromising student rights to privacy.

Academic Libraries and FERPA and SEVIS: The Family Educational Rights and Privacy Act (FERPA) was passed to protect the privacy of student education records and to define who can access these records. FERPA grants parents the rights until the child turns 18 years old or attends a school beyond the high school level. The Student and Exchange Visitors Information System (SEVIS) maintains updated information on approximately one million non-immigrant foreign students and exchange visitors during the course of their stay in the United States each year. Colleges and universities are now required to report a foreign student's failure to enroll or if students drop out of their programs. Colleges and university librarians need to identify how their institutions implement these laws and whether they have any impact on the collection and retention of library user records.

Academic Libraries and Faculty: Academic institutions often rely on principles of academic freedom to protect the intellectual freedom of faculty. While the principles of academic freedom are intended to protect faculty from professional consequences of researching in unpopular or controversial areas, they do not necessarily protect the privacy of faculty. Academic libraries should also have in place appropriate policies based on First Amendment and Fourth Amendment rights to protect the privacy of faculty members' library records.

Academic Libraries and Computer Systems: The computer networks of academic libraries are often part of institutional networks, under the ultimate control of units outside the library. Academic libraries should work with campus computer departments to ensure that student and faculty information-seeking activity is kept confidential and well protected throughout the institution. In addition, library personnel should review library procedures and arrangements with outside vendors to ensure the highest level of protection for such records as online digital reference logs, proxy server and other authentication devices, e-mail reference transactions, personalized searching, and SDI profiles.

Selected Links:

- Barbara M. Jones, "Academic Libraries and Intellectual Freedom" http://www.ifmanual.org/alif
- United States Department of Education, Family Educational Rights and Privacy Act (FERPA) http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

School Libraries

School library media specialists have an ethical obligation to protect and promote student privacy. Although the educational level and program of the school necessarily shapes the resources and services of a school library, the principles of the Library Bill of Rights apply equally to all librarians, including school library media specialists.

School Libraries and FERPA: School records are governed by the Family Educational Rights and Privacy Act (FERPA) that grants parents the rights to access student educational records until the child turns 18 years old. School library media specialists need to identify how their institutions implement this law and its impact on collection and retention of library user records.

Students as Library Users: Students who use school libraries need to learn about the concepts of privacy and confidentiality. They may not know the dangers of sharing personally identifiable information with others. School library media specialists may face the situation of an adult asking for information pertaining to students' library use. These situations must be handled in accordance with all school and library policies. In an ideal situation, that information would not be released. Teachers should not be able to "check" on students to see if they have borrowed assigned readings or used specific resources. School library media specialists are best served when they assist teachers in developing classroom procedures and policies that preserve user privacy and meet educational goals.

School Library Procedures: School library media specialists have a responsibility to "assume a leadership role in promoting the principles of intellectual freedom within the school by providing resources and services that create and sustain an atmosphere of free inquiry." This includes safeguarding student and teacher privacy. School library personnel must strive to: educate all members of the school community about the value of privacy to school library media center users; develop board approved policies that provide the highest level of protection for all records; and, teach all members of the educational community about the policies and procedures that govern privacy. School libraries operate as part of larger educational structures. In some cases school systems may create policies and procedures that infringe on students' rights to privacy. School library personnel are encouraged to educate all policy makers about the dangers of abridging students' privacy rights.

School libraries and COPPA: The Children's Online Privacy Protection Act (COPPA) directly affects commercial Web sites targeted to children, as well as those sites that know they are collecting personally identifiable information from children 12 and under. Such sites have a legal obligation to comply with the law. Prosecution is one of the penalties for non-compliance. Noncommercial Web sites, such as library, nonprofit, community groups, and government agencies are not covered by COPPA. A library collecting personal information from children in order to e-mail them summer reading lists or reference assistance is not required to seek parental consent. Although libraries are not directly impacted by COPPA, children using the Internet in a library may need help understanding the law and getting consent from their parents. In some instances, children will find that COPPA may restrict their ability to participate in some activities on Web sites while they await parental approval. It is the librarians' role to guide children through the process or help them find alternative activities online. Parents may need assistance in understanding the law and the significance of the requests they receive from Web sites. Librarians and libraries should play a key role in helping all library users understand and comply with COPPA. (*Note: The extent to which schools can or do assume parental responsibilities for students will depend in large part on decisions made by the local school board or superintendent. It will also depend on the nature of the resources being used in the classroom and whether those resources require students to divulge personally identifiable information. Some schools may decide to act on behalf of the child, others may decide to seek consent through an Acceptable Use Policy signed by students and parents at the beginning of the year, while others may take no responsibility at all and leave it up to parents. However the school implements the law, it must take care not to allow COPPA to interfere with curricular decisions.)*

Selected Links:

- American Association of School Librarians, Position Statement on the Confidentiality of Library Records http://www.ala.org/aasl/advocacy/resources/position-statements/library-records
- Selected Testimonies to the Child Online Protection Act Commission http://www.ala.org/offices/oif/ifissues/issuesrelatedlinks/slctedtestimonies
- United States Department of Education, Family Policy Compliance Office Web Site

Public Library Services to Minors

The rights of minors vary from state to state. Libraries may wish to consult the legal counsel of their governing authorities to ensure that policy and practice are in accord with applicable law. In addition, the legal responsibilities and standing of library staff in regard to minors differ substantially in school and public libraries. In all instances, best practice is to extend to minors the maximum allowable confidentiality and privacy protections.

The Children's Online Privacy Protection Act (COPPA) requires commercial Web sites that collect personally identifiable information from children 12 and under to obtain consent from their parents or guardians in advance. COPPA was written with three parties in mind: parents, children, and commercial Web sites. Although COPPA does not place any special obligations on public libraries, there are two impacts to consider:

1. When children use internet access in libraries, library staff need to be able to explain COPPA's effects to children and their parents.
2. When a library designs Web pages and services for children, it may wish to provide the same privacy protections as the protections mandated for commercial Web sites.

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 minor children about those choices. Librarians should not breach a minor's confidentiality by giving out information readily available to the parent from the minor directly. Libraries should take great care to limit the extenuating circumstances in which they release such information.

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.

The rights of minors to privacy regarding their choice of library materials should be respected and protected.

IV. Questions to Ask When Drafting Privacy and Confidentiality Policies and Procedures

Policy drafts should be reviewed against existing local policies, state and local legislation, and ALA recommendations and guidelines. It may also help policy drafting teams and trainers to ask themselves and their staff questions from the checklists below, considering how and whether policies and procedures under consideration provide appropriate guidance. Common privacy- or confidentiality-violating scenarios are also available for use in training or policy review.

Sources:

- Carolyn Caywood, "Questions and Answers about Privacy in Libraries," presented at the Virginia Library Association 2002 Conference, October 17, 2002.
- "Confidentiality Inventory," in Confidentiality in Libraries: An Intellectual Freedom Modular Education Program Trainer's Manual (Chicago: ALA, 1993), p. 30.
- Barbara Jones, "Intellectual Freedom Policies for Privacy," Libraries, Access, and Intellectual Freedom: Developing Policies for Public and Academic Libraries (Chicago: ALA, 1999), p. 147-168.
- Confidentiality in Libraries: An Intellectual Freedom Modular Education Program Trainer's Manual (Chicago: ALA, 1993).

Checklist of Basic Questions about Privacy and Confidentiality

Collecting Information

□ Do we need to know this to operate the library?

□ How long do we need to know it?

□ How will we protect what we collect?

□ How will we destroy what we collect?

□ How will we inform the public about confidentiality?

□ How will we give users choices?

□ How will we inform/influence government acts that impact confidentiality?

Providing Privacy

□ Where do users need privacy to protect their intellectual freedom?

□ Where would privacy endanger safety?

□ How will we provide privacy where we should?

□ How will we ensure safety without being intrusive?

□ How will we educate staff about privacy?

□ How will we inform the public about privacy in libraries?

□ How will we inform the public about library resources on privacy issues?

□ How will we give users choices?

Reviewing Your Policy

□ Does your policy statement explain the difference between privacy and confidentiality in a library setting?

□ Does your statement make clear the role of confidentiality in protecting intellectual freedom?

□ Is the information to be protected listed: reference requests, information services, circulation & registration records, server and client computer logs?

□ Have you included language to deal with unforeseen circumstances, like "including, but not limited to . . ."?

□ Does your policy require that library users be notified whenever their PII is collected by the library and be told how to correct inaccurate information?

□ Do you state who may or may not have access to patron information?

□ Do you outline the specific conditions under which access may be granted? i.e., with a court order after good cause has been demonstrated?

□ Do you list the procedure for adopting the policy?

□ Are there provisions for notifying the public of the policy?

□ Are exemptions, exceptions, or special conditions enumerated?

□ Do you address needs unique to your library environment?

□ If your library is part of a cooperative, automated library system, are there provisions for coordination with the other libraries in your system?

□ Is the procedure outlined for responding to court orders of various types?

□ Are the Library Bill of Rights, Statement on Professional Ethics, ALA Policy on the Confidentiality of Library Records, and state & local laws (where applicable) mentioned or acknowledged? Does your policy conform to these supporting documents?

ALA Guidelines for Developing a Library Privacy Policy

Appendix 1

Model Privacy Policy

(*Note: This document represents an ideal privacy policy and should be used in conjunction with the ALA Guidelines for Developing a Library Privacy Policy. Many elements may not pertain to all libraries. Each section should be reviewed to reflect local policies and practices.*)

I. Introduction

Privacy is essential to the exercise of free speech, free thought, and free association. In this library the right to privacy is the right to open inquiry without having the subject of one's interest examined or scrutinized by others. Confidentiality exists when a library is in possession of personally identifiable information about users and keeps that information private on their behalf.

The courts have upheld the right to privacy based on the Bill of Rights of the U.S. Constitution. Many states provide guarantees of privacy in their constitutions and statute law. Numerous decisions in case law have defined and extended rights to privacy. This library's privacy and confidentiality policies are in compliance with applicable federal, state, and local laws.

User rights—as well as our institution's responsibilities—outlined here are based in part on what are known in the United States as the five "Fair Information Practice Principles." These five principles outline the rights of Notice, Choice, Access, Security, and Enforcement.

Our commitment to your privacy and confidentiality has deep roots not only in law but also in the ethics and practices of librarianship. In accordance with the American Library Association's Code of Ethics:

"We protect each library user's right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired, or transmitted."

II. [Your Institution's Name] Commitment to Our Users Rights of Privacy and Confidentiality

This privacy policy explains your privacy and confidentiality rights, the steps this library takes to respect and protect your privacy when you use library resources, and how we deal with personally identifiable information that we may collect from our users.

1. Notice & Openness

We affirm that our library users have the right of "notice"—to be informed about the policies governing the amount and retention of personally identifiable information, and about why that information is necessary for the provision of library services.

We post publicly and acknowledge openly the privacy and information-gathering policies of this library. Whenever policies change, notice of those changes is disseminated widely to our users.

In all cases we avoid creating unnecessary records, we avoid retaining records not needed for the fulfillment of the mission of the library, and we do not engage in practices that might place information on public view.

Information we may gather and retain about current and valid library users include the following (This list should be comprehensive, and should include locally relevant examples):

- User Registration Information
- Circulation Information
- Electronic Access Information
- Information Required to Provide Library Services

2. Choice & Consent

This policy explains our information practices and the choices you can make about the way the library collects and uses your information. We will not collect or retain your private and personally identifiable information without your consent. Further, if you consent to give us your personally identifiable information, we will keep it confidential and will not sell, license or disclose personal information to any third party without your consent, unless we are compelled to do so under the law or to comply with a court order.

If you wish to receive borrowing privileges, we must obtain certain information about you in order to provide you with a library account. When visiting our library's Web site and using our electronic services, you may choose to provide your name, e-mail address, library card barcode, phone number or home address.

You have the option of providing us with your e-mail address for the purpose of notifying you about your library account. You may request that we remove your e-mail address from your record at any time.

We never use or share the personally identifiable information provided to us online in ways unrelated to the ones described above without also providing you an opportunity to prohibit such unrelated uses, unless we are compelled to do so under the law or to comply with a court order.

(For academic libraries) If you are affiliated with our university, the library automatically receives personally identifiable information to create and update your library account from the Registrar's Office (for students) or Human Resources (for employees).

3. Access by Users

Individuals who use library services that require the function and process of personally identifiable information are entitled to view and/or update their information. You may either view or update your personal information online or in person. In both instances, you may be asked to provide some sort of verification such as a pin number or identification card to ensure verification of identity.

The purpose of accessing and updating your personally identifiable information is to ensure that library operations can function properly. Such functions may include notification of overdue items, recalls, reminders, etc. The library will explain the process of accessing or updating your information so that all personally identifiable information is accurate and up to date.

4. Data Integrity & Security

Data Integrity: The data we collect and maintain at the library must be accurate and secure. We take reasonable steps to assure data integrity, including: using only reputable sources of data; providing our users access to your own personally identifiable data; updating data whenever possible; utilizing middleware authentication systems that authorize use without requiring personally identifiable information; destroying untimely data or converting it to anonymous form.

Data Retention: We protect personally identifiable information from unauthorized disclosure once it is no longer needed to manage library services. Information that should be regularly purged or shredded includes personally identifiable information on library resource use, material circulation history, and security/surveillance tapes and logs.

Tracking Users: We remove links between patron records and materials borrowed when items are returned and we delete records as soon as the original purpose for data collection has been satisfied. We permit in-house access to information in all formats without creating a data trail. Our library has invested in appropriate technology to protect the security of any personally identifiable information while it is in the library's custody, and we ensure that aggregate, summary data is stripped of personally identifiable information. We do not ask library visitors or Web site users to identify themselves or reveal any personal information unless they are borrowing materials, requesting special services, registering for programs or classes, or making remote use from outside the library of those portions of the Library's Web site restricted to registered borrowers under license agreements or other special arrangements. We discourage users from choosing passwords or PINs that could reveal their identity, including social security numbers. We regularly remove cookies, Web history, cached files, or other computer and Internet use records and other software code that is placed on our computers or networks.

Third Party Security: We ensure that our library's contracts, licenses, and offsite computer service arrangements reflect our policies and legal obligations concerning user privacy and confidentiality. Should a third party require access to our users' personally identifiable information, our agreements address appropriate restrictions on the use, aggregation, dissemination, and sale of that information, particularly information about minors. In circumstances in which there is a risk that personally identifiable information may be disclosed, we will warn our users. When connecting to licensed databases outside the library, we release only information that authenticates users as "members of our community." Nevertheless, we advise users of the limits to library privacy protection when accessing remote sites

Cookies: Users of networked computers will need to enable cookies in order to access a number of resources available through the library. A cookie is a small file sent to the browser by a Web site each time that site is visited. Cookies are stored on the user's computer and can potentially transmit personal information. Cookies are often used to remember information about preferences and pages visited. You can refuse to accept cookies, can disable cookies, and remove cookies from your hard drive. Our Library servers use cookies solely to verify that a person is an authorized user in order to allow access to licensed library resources and to customize Web pages to that user's specification. Cookies sent by our Library servers will disappear when the user's computer browser is closed. We will not share cookies information with external third parties.

Security Measures: Our security measures involve both managerial and technical policies and procedures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data. Our managerial measures include internal organizational procedures that limit access to data and ensure that those individuals with access do not utilize the data for unauthorized purposes. Our technical security measures to prevent unauthorized access include encryption in the transmission and storage of data; limits on access through use of passwords; and storage of data on secure servers or computers that are inaccessible from a modem or network connection.

Staff access to personal data: We permit only authorized Library staff with assigned confidential passwords to access personal data stored in the Library's computer system for the purpose of performing library work. We will not disclose any personal data we collect from you to any other party except where required by law or to fulfill an individual user's service request. The Library does not sell or lease users' personal information to companies, universities, or individuals.

5. Enforcement & Redress

Our library will not share data on individuals with third parties unless required by law. We conduct regular privacy audits in order to ensure that all library programs and services are enforcing our privacy policy. Library users who have questions, concerns, or complains about the library's handing of their privacy and confidentiality rights should file written comments with the Director of the Library. We will respond in a timely manner and may conduct a privacy investigation or review of policy and procedures.

We authorize only the Library Director and our Library Privacy Officer to receive or comply with requests from law enforcement officers; we confer with our legal counsel before determining the proper response. We will not make library records available to any agency of state, federal, or local government unless a subpoena, warrant, court order or other investigatory document is issued by a court of competent jurisdiction that shows good cause and is in proper form. We have trained all library staff and volunteers to refer any law enforcement inquiries to library administrators.