

Privacy Tool Kit

Privacy is essential to the exercise of free speech, free thought, and free association. Lack of privacy and confidentiality chills users' choices, thereby suppressing access to ideas. The possibility of surveillance, whether direct or through access to records of speech, research and exploration, undermines a democratic society.—*Privacy: An Interpretation of the Library Bill of Rights*

Table of Contents

Introduction	2
Privacy Policy	9
Guidelines for Developing a Library Privacy Policy	17
Privacy Procedures	41
Privacy Communication	43
Crisis Communication.....	44
Messages/Talking Points.....	49
Tips for Ensuring Privacy	52
Legislative Advocacy.....	55
Select Bibliography	57

Contributors

[American Library Association Office for Intellectual Freedom](#)

Permission is granted to libraries to reproduce the Privacy Tool Kit.
May 2, 2005

Privacy Tool Kit

<http://www.ala.org/ala/oif/iftoolkits/toolkitsprivacy/privacy.htm>

INTRODUCTION

Background: Privacy is essential to the exercise of free speech, free thought, and free association. Lack of privacy and confidentiality chills users' choices, thereby suppressing access to ideas. The possibility of surveillance, whether direct or through access to records of speech, research and exploration, undermines a democratic society.

Confidentiality of library records is a core value of librarianship. One cannot exercise the right to read if the possible consequences include damage to one's reputation, ostracism from the community or workplace, or criminal penalties. Choice requires both a varied selection and the assurance that one's choice is not monitored.

For libraries to flourish as centers for uninhibited access to information, librarians must stand behind their users' right to privacy and freedom of inquiry. Just as people who borrow murder mysteries are unlikely to be murderers, so those seeking information about terrorism are unlikely to be terrorists. Assuming a sinister motive based on library users' reading choices makes no sense and leads to fishing expeditions that both waste precious law enforcement resources and have the potential to chill Americans' inquiry into current events and public affairs.

The right to privacy is the right to open inquiry without having the subject of one's interest examined or scrutinized by others. Confidentiality relates to the possession of personally identifiable information, including such library-created records as closed-stack call slips, computer sign-up sheets, registration for equipment or facilities, circulation records, Web sites visited, reserve notices, or research notes.

History of ALA's efforts to protect privacy and confidentiality: Historically, librarians have sought to protect users' confidentiality by scrupulously guarding library patrons' records from public scrutiny. ALA first officially recognized the right to privacy in 1939 in its Code of Ethics for Librarians. Today, the ALA professional ethics code continues to acknowledge the paramount importance of library patron privacy:

[ALA Code of Ethics](http://www.ala.org/ala/oif/policies/codeofethics) (first passed, 1939, rev. 1995)

(<http://www.ala.org/ala/oif/policies/codeofethics>)

"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."

[ALA Library Bill of Rights](http://www.ala.org/ala/oif/policies/librarybillrights) (1948, amended 1961, 1980, reaffirmed 1996)

(<http://www.ala.org/ala/oif/policies/librarybillrights>)

"The right to privacy in a library is implicit in ALA's Library Bill of Rights, which guarantees free access to library resources for all users and opposes any limitations on the right to an individual's exercise of free expression."

Through the *Library Bill of Rights* and the *ALA Code of Ethics*, librarians fight to protect patron privacy and preserve our democratic society by promoting a diversity of viewpoints and ideas to support an informed, literate, and educated public.

After World War II, government officials, law enforcement officers, journalists, and others sought to obtain information from librarians about reading habits and other library usage. The second half of the century saw an increasing number and frequency of challenges to the confidentiality concerns of librarians, including:

- 1980s, the FBI and/or local law enforcement agencies seek information about library users.
- 1990's–date, Internet use prompts investigations about users' electronic inquiries in libraries.
- 2001-date, adoption of the [USA PATRIOT Act](#) and related actions authorizes law enforcement officials to seek library records without probable cause.
- 2002-date, new federal data mining programs like the [Total Information Awareness Program](#) (TIA) (<http://www.ala.org/oif/ifissues/surveillanceinamerica>)—now called the [Terrorism Information Awareness Program](#) (<http://www.ala.org/oif/ifissues/tia>)—in the Defense Department, the CAPPS II no fly list database, and the proposed Terrorism Information and Prevention System (TIPS) alarm librarians about potential covert use of library records.

Recent ALA Actions to Protect Privacy: ALA first adopted a statement specifically about confidentiality of library records in 1971. This statement was modified in the late 1980's to respond to concerns about visits from the FBI and other law enforcement officials. Most states either passed or modified their laws to protect the confidentiality of library records. But with the advent of new technologies, these guarantees were not enough.

In 1999, the ALA Council asked the Library and Information Technology Association (LITA) to examine the impact of new technologies on patron privacy and the confidentiality of electronic records. In July 2000, ALA Council approved the [LITA Final Report of the Task Force on Privacy and Confidentiality in the Electronic Environment](#) (<http://www.ala.org/ala/lita/litaresources/taskforceonpriv/alataskforce.htm>) and referred it to the Intellectual Freedom Committee (IFC) for review. LITA recommended that:

1. ALA revise its policy statements related to [Confidentiality of Library Records](#) (rev. 1986) (<http://www.ala.org/Template.cfm?Section=otherpolicies&Template=/ContentManagement/ContentDisplay.cfm&ContentID=13084>), and [Concerning Confidentiality of Personally Identifiable Information About Library Users](#) (1991) (<http://www.ala.org/Template.cfm?Section=otherpolicies&Template=/ContentManagement/ContentDisplay.cfm&ContentID=13087>), in order to specifically and appropriately incorporate Internet privacy.
2. ALA develop model privacy policies, instructional materials, and privacy "best practices" documents for libraries; and
3. ALA urge that all libraries adopt a privacy statement on Web pages and post privacy policies in the library which cover the issues of privacy in Internet use as accessed through the library's services.

In 2001, the IFC established a standing Privacy Subcommittee to monitor ongoing privacy developments in technology, public policy, and legislation and to identify needs and resources for librarians and library users. In June, 2002, ALA Council adopted IFC's [Privacy: An Interpretation of the Library Bill of Rights](#) (<http://www.ala.org/oif/policies/interpretations/privacy>), affirming that, "Privacy is essential to the exercise of free speech, free thought, and free association" and "in a library (physical or virtual), the right to privacy is the right to open inquiry without having the subject of one's interest examined or scrutinized by others." The IFC then drafted "[Questions and Answers about Privacy and Confidentiality](#)" (<http://www.ala.org/oif/policies/interpretations/privacyqanda>), to help ALA members respond to the numerous challenges raised daily. Also in 2002, the ALA Council adopted a document drafted by the Office of Technology Policy entitled, "[Principles for the Networked World](#)"

(<http://www.ala.org/ala/washoff/washpubs/principles.pdf>)," which defines and establishes principles about privacy as follows:

Privacy: The freedom to choose the degree to which personal information is monitored, collected, disclosed, and distributed.

Principles:

1. Privacy is a right of all people and must be protected in the networked world.
2. The rights of anonymity and privacy while people retrieve and communicate information must be protected as an essential element of intellectual freedom.
3. The long-established principles of [Fair Information Practices](#) (http://www.epic.org/privacy/consumer/code_fair_info.html) that underlie U.S. and many other national privacy laws must be at the core of privacy policies in the networked world.
4. Users have the right to be fully informed about privacy policies and principles in the networked world.
5. Library patron confidentiality must be protected by law and policy.

The Privacy Tool Kit: This [Privacy Tool Kit](#) (<http://www.ala.org/oif/iftoolkits/privacy>) is designed to assist libraries and librarians in understanding privacy and its relationship to information access in libraries, and to provide action tools that apply to their local circumstances. It pulls together the statements, policies and other documentation previously prepared by ALA as well as several additional topics, including:

- Background documents about the right to privacy and the need to preserve it;
- Actions that you, your library, and your library association can take;
- [Guidance on developing a privacy policy](#) (<http://www.ala.org/oif/iftoolkits/privacy/guidelines>)
- A model privacy policy;
- Conducting a privacy audit;
- Federal privacy laws;
- State laws protecting the confidentiality of library records;
- Law enforcement warrants, subpoenas, and other orders for library records;
- Guidelines for coping with law enforcement inquiries;
- Procedures for implementing privacy policies;
- Communications guidelines;
- Legislative advocacy;
- Privacy Guidelines for Library Users; and
- Bibliography

The Right to Privacy

The right to privacy is an intrinsic American value. Although the Constitution does not explicitly reference the word "privacy," the Supreme Court has nonetheless inferred a right to privacy from various portions of the Bill of Rights and the common law.

The most obvious protection of privacy in the Bill of Rights is the [Fourth Amendment](#) (<http://www.ala.org/Template.cfm?Section=issuesrelatedlinks&Template=/ContentManagement/ContentDisplay.cfm&ContentID=25291>), which protects individuals "in their persons, homes, papers, and effects

from unreasonable searches and seizures" by the government. The [First Amendment](http://www.ala.org/alaorg/oif/first.html) (<http://www.ala.org/alaorg/oif/first.html>), which protects freedom of religion, speech, press, and assembly, also implicitly safeguards the right to privacy in the form of freedom of thought and intellect. In recent years, several federal courts have found that the First Amendment protects the right to receive information in a publicly funded library.

The Fourth Amendment and Privacy in Libraries:

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

Along with the First Amendment, the Fourth Amendment provides a Constitutional basis for protecting the privacy of library users. This amendment has mixed origins including British legal theory recognizing that a "man's house is his castle," British polices that authorized general searches, and colonial outrage concerning the Crown's use of general warrants to gain evidence to maximize royal revenues and for political purposes. Even after the Declaration of Independence, some states violated the privacy of individuals for political purposes. For example, in 1777 in Pennsylvania the homes of Quakers who had not taken an oath of allegiance to the United States were searched. Books and papers were seized; more than forty people were arrested and deported without trial to Virginia where they were held until the next year.

Modern Fourth Amendment law relies heavily on [Katz v. United States](http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&vol=389&invol=347) (<http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&vol=389&invol=347>), 389 U.S. 347 (1967) in which the Court held that the Fourth amendment "protects people, not places" and what a person "seeks to preserve as private, even in area accessible to the public, may be constitutionally protected". The two-part test most often used by the Court to determine whether a right to privacy exists was expressed by Justice Harlan in his concurrence to Katz: 1) a person has "exhibited an actual (subjective) expectation of privacy" and 2) that the expectation is "one that society is prepared to recognize as 'reasonable.'"

In the Katz decision the Court also reiterated that, "the person's general right to privacy—his right to be let alone by other people—is like the protection of his property and of his very life, left largely to the law of the individual states." Thus, it is important that librarians be aware of the legal standard for determining privacy rights under their state law. For instance, in Washington state a person's "right to privacy," "right of privacy," "privacy," or "personal privacy," ... is invaded or violated only if disclosure of information about the person: (1) would be highly offensive to a reasonable person, and (2) is not of legitimate concern to the public (RCW 42.17.255).

Selected Sources:

- Solove, Daniel J. and Marc Rotenberg (2003). Information Privacy Law. New York: Aspen Publishers.
- Levy, Leonard E. "The Fourth Amendment: Search and Seizure," in Origin of the Bill of Rights, (New Haven: Yale University Press, 1999): 150 – 179.

Other Constitutional and International Agreements that Protect Privacy: Beyond the First and Fourth Amendments, the [Fifth Amendment](http://www.ala.org/Template.cfm?Section=issuesrelatedlinks&Template=/ContentManagem) (<http://www.ala.org/Template.cfm?Section=issuesrelatedlinks&Template=/ContentManagem>

ent/ContentDisplay.cfm&ContentID=25291) guarantees against self-incrimination, and the [Ninth Amendment](#) (<http://www.ala.org/Template.cfm?Section=issuesrelatedlinks&Template=/ContentManagement/ContentDisplay.cfm&ContentID=25291>) guarantees that "[t]he enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people." This right is also explicit in Article Twelve of the [Universal Declaration of Human Rights](#) (<http://www.un.org/Overview/rights.html>): "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." This right has further been explicitly codified as Article Seventeen of the "[International Covenant on Civil and Political Rights](#)" (http://www.unhchr.ch/html/menu3/b/a_ccpr.htm), a legally binding international human rights agreement ratified by the United States on June 8, 1992.

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](#) (<http://www.ala.org/oif/stateprivacylaws>), and the attorneys general in the remaining two states have issued opinions recognizing the privacy of users' library records. Cases recognizing a right to privacy include: [NAACP v. Alabama](#) (<http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&vol=357&invol=449>), 357 U.S. 449 (1958); [Griswold v. Connecticut](#) (<http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&vol=381&invol=479>) 381 U.S. 479 (1965); [Katz v. United States](#) (<http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&vol=389&invol=347>), 389 U.S. 347 (1967); and [Stanley v. Georgia](#) (<http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=394&invol=557>), 394 U.S. 557 (1969). Congress recognized the right to privacy in the [Privacy Act of 1974](#) (<http://www.usdoj.gov/foia/privstat.htm>) and Amendments (5 USC Sec. 552a), which addresses the potential for government's violation of privacy through its collection of personal information. The Privacy Act's "Congressional Findings and Statement of Purpose" state in part: "the right to privacy is a personal and fundamental right protected by the Constitution of the United States." See: [Section 552a. Records maintained on individuals](#) (http://caselaw.lp.findlaw.com/scripts/ts_search.pl?title=5&sec=552a).

What You, Your Library and Your Library Associations Should Do to Protect Privacy

- Limit the degree to which personally identifiable information is monitored, collected, disclosed, and distributed.
- Avoid creating unnecessary records. Only record a user's personally identifiable information when necessary for the efficient operation of the library.
- Avoid retaining records that are not needed for efficient operation of the library. Assure that all kinds and types of records are covered by the policy, including data-related logs, digital records, vendor-collected data, and system backups.
- Avoid library practices and procedures that place information on public view (e.g., using postcards for overdue notices or requested materials; using patron names to identify self-pickup holds; placing staff terminals so the screens can be read by the public; using sign-in sheets to use computers or other devices; and providing titles of reserve requests or interlibrary loans over the telephone to users' family members or answering machines).

Actions to Take Within Local Libraries

- Educate staff, trustees, volunteers, and contract workers on a continuous basis about library privacy principles, policies and procedures, and library staff's legal and ethical responsibilities as custodians of personally identifiable information.
- Inform library staff about their responsibility to cooperate with other organizations that work to protect privacy and challenge intrusions.
- Educate the public through a variety of learning methods that provide the information and tools individuals need to protect their privacy and the confidentiality of their own personally identifiable information.
- Create and publicize a local [privacy policy](http://www.ala.org/ala/oif/ifttoolkits/toolkitsprivacy/privacypolicy/privacypolicy.htm) (<http://www.ala.org/ala/oif/ifttoolkits/toolkitsprivacy/privacypolicy/privacypolicy.htm>), using the recommendations and resources made available through the Privacy Tool Kit. Include all aspects of services including protection of electronic data and dissemination of electronic records. Implement a privacy audit process to assure that an organization's goals and promises of privacy and confidentiality are supported by its practices, thereby protecting confidential information from abuse and the organization from liability and public relations problems.
- Ensure that contracts and licenses reflect library policies and legal obligations concerning user privacy and confidentiality; make sure the agreements address appropriate restrictions on the use, aggregation, dissemination, and sale of personally identifiable information, particularly information about minors.
- Extend to [minors](http://www.ala.org/ala/oif/statementspols/statementspolicies.htm#minors) (<http://www.ala.org/ala/oif/statementspols/statementspolicies.htm#minors>) the maximum allowable confidentiality and privacy protections.
- Notify parents about the library's privacy and confidentiality policies when issuing library cards to minors.
- Educate children, parents, students, teachers and school and college officials about the [Children's Online Privacy Protection Act](#) (COPPA) (<http://www.ftc.gov/bcp/online/edcams/coppa/intro.htm>) and the [Family Educational Rights and Privacy Act](#) (FERPA) (<http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html>). COPPA requires commercial Web sites to obtain parental permission before collecting information from children under 13. FERPA requires educational institutions to protect students' privacy with regard to educational records.

Actions to Take Within States

- Ensure that [state privacy and confidentiality laws](http://www.ala.org/oif/stateprivacylaws) (<http://www.ala.org/oif/stateprivacylaws>) are up-to-date and readily available to library staff and users. Note: Privacy rights of minors differ from state to state.
- Invite privacy specialists to speak and conduct workshops at local and state chapter conferences.
- Publicize the need for libraries to adopt privacy policies in state chapter journals and other communications vehicles.
- Develop [alliances](http://www.ala.org/Template.cfm?Section=basicrelatedlinks&Template=/ContentManagement/ContentDisplay.cfm&ContentID=11699) (<http://www.ala.org/Template.cfm?Section=basicrelatedlinks&Template=/ContentManagement/ContentDisplay.cfm&ContentID=11699>) with other state-wide groups advocating for privacy rights.
- Monitor and advocate for [legislation](http://www.ala.org/ala/oif/basics/basicrelatedlinks/contactingelected.htm) (<http://www.ala.org/ala/oif/basics/basicrelatedlinks/contactingelected.htm>) that protects user privacy.

Actions to Take Within ALA

- Create and update policies and procedures about privacy and confidentiality (<http://www.ala.org/oif/policies>).
- Represent libraries in federal policy making and court proceedings.
- Develop tools to help libraries ensure privacy and confidentiality.
- Work with other organizations concerned with free expression and privacy concerns (<http://www.ala.org/ala/oif/firstamendment/advocates/advocates.htm>).
- Monitor developments in the privacy arena.
- Assist libraries with legal actions.
- Provide guidance and other assistance when library privacy is challenged.
- Advocate for the public's information rights related to access, free expression and privacy.
- Provide specific guidance related to the Children's Online Privacy Protection Act (<http://www.ftc.gov/bcp/online/pubs/buspubs/coppa.htm>).

Privacy Tool Kit

[Return to the Privacy Tool Kit](#)

PRIVACY POLICY

American Library Association Privacy Policies and Statements

The American Library Association has developed policies, guidelines, and resources to assist librarians in preserving privacy and confidentiality for library users.

Basic Statements

[Library Bill of Rights](#) (1948, amended 1961, 1980, reaffirmed 1996)
(<http://www.ala.org/oif/policies/librarybillrights>)

[Freedom to Read Statement](#) (1953; rev. 1972, 1991, 2000)
(<http://www.ala.org/oif/policies/freedomtoread>)

[Code of Ethics](#) (rev. 1995) (<http://www.ala.org/oif/policies/codeofethics>)

[Freedom to View Statement](#) (1990) (<http://www.ala.org/oif/policies/freedomtoview>)

[Library Principles for a Networked World](#) (2002)
(<http://www.ala.org/ala/washoff/washpubs/principles.pdf>)

Privacy and Confidentiality Policies and Procedures

[Policy on Confidentiality of Library Records](#) (1971; rev. 1975, 1986)
(<http://www.ala.org/Template.cfm?Section=otherpolicies&Template=/ContentManagement/ContentDisplay.cfm&ContentID=13084>)

[Suggested Procedures for Implementing Policy on Confidentiality of Library Records](#) (1983; rev. 1988)
(<http://www.ala.org/Template.cfm?Section=otherpolicies&Template=/ContentManagement/ContentDisplay.cfm&ContentID=20013>)

[Privacy: An Interpretation of the Library Bill of Rights](#) (2002)
(<http://www.ala.org/oif/policies/interpretations/privacy>)

[Questions and Answers on Privacy and Confidentiality](#) (2003)
(<http://www.ala.org/oif/policies/interpretations/privacyqanda>)

[Privacy Resources for Librarians, Library Users, and Families](#) (last updated 2002)
(<http://www.ala.org/ala/oif/ifissues/issuesrelatedlinks/privacyresources.htm>)

[Guidelines for Developing a Library Privacy Policy](#) (August 2003; rev. March 2005)
(<http://www.ala.org/oif/iftoolkits/privacy/guidelines>)

[ALA Issues New Guidelines for Developing Library Privacy Policy](http://www.ala.org/ala/pressreleasesbucket/pressreleases2003sep/alaissuesnew.htm) (September 19, 2003)
(<http://www.ala.org/ala/pressreleasesbucket/pressreleases2003sep/alaissuesnew.htm>)

[Developing a Confidentiality Policy](http://www.ala.org/Template.cfm?Section=Dealing_with_Challenges&Template=/ContentManagement/ContentDisplay.cfm&ContentID=11165) (from ALA, Intellectual Freedom Manual, 6th edition, Chicago, IL: American Library Association, Office for Intellectual Freedom, 2002:347-355)
(http://www.ala.org/Template.cfm?Section=Dealing_with_Challenges&Template=/ContentManagement/ContentDisplay.cfm&ContentID=11165)

[Policy concerning Confidentiality of Personally Identifiable Information about Library Users](http://www.ala.org/Template.cfm?Section=otherpolicies&Template=/ContentManagement/ContentDisplay.cfm&ContentID=13087) (1991)
(<http://www.ala.org/Template.cfm?Section=otherpolicies&Template=/ContentManagement/ContentDisplay.cfm&ContentID=13087>)

[AASL Position Statement on the Confidentiality of Library Records](http://www.ala.org/ala/aasl/aaslproftools/positionstatements/aaslpositionstatementconfidentiality.htm) (Rev. July 1999)
(<http://www.ala.org/ala/aasl/aaslproftools/positionstatements/aaslpositionstatementconfidentiality.htm>)

[ALA Task Force on Privacy and Confidentiality in the Electronic Environment Final Report](http://www.ala.org/ala/lita/litaresources/alataskforce.htm) (July 2000)
(<http://www.ala.org/ala/lita/litaresources/alataskforce.htm>).

[Appendix addressing new technologies related to: Confidentiality of Library Records. Usage Tracking. Security Issues. Institutional Concerns and Developments. Library Practices. Commercial Applications](http://www.ala.org/ala/lita/litaresources/taskforceonpriv/appendix.htm)
(<http://www.ala.org/ala/lita/litaresources/taskforceonpriv/appendix.htm>)

[The Children's Online Privacy Protection Act](http://www.ala.org/ala/washoff/WOissues/civilliberties/coppa/Default2434.htm)
(<http://www.ala.org/ala/washoff/WOissues/civilliberties/coppa/Default2434.htm>)

[Privacy Legislation](http://www.ala.org/ala/washoff/WOissues/civilliberties/privacy/privacyrelated.htm) (<http://www.ala.org/ala/washoff/WOissues/civilliberties/privacy/privacyrelated.htm>)

[Libraries and The Patriot Act Legislation](http://www.ala.org/Template.cfm?Section=issuesrelatedlinks&Template=/ContentManagement/ContentDisplay.cfm&ContentID=46741)
(<http://www.ala.org/Template.cfm?Section=issuesrelatedlinks&Template=/ContentManagement/ContentDisplay.cfm&ContentID=46741>)

[State Privacy Laws regarding Library Records](http://www.ala.org/oif/stateprivacylaws) (<http://www.ala.org/oif/stateprivacylaws>)

Policies and Statements about the Infringement of Users' Privacy Rights

[USA Patriot Act](http://www.ala.org/ala/oif/ifissues/usapatriotact.htm) (<http://www.ala.org/ala/oif/ifissues/usapatriotact.htm>)

[Resolution on the USA Patriot Act and Related Measures That Infringe on the Rights of Library Users](http://www.ala.org/Template.cfm?Section=ifresolutions&Template=/ContentManagement/ContentDisplay.cfm&ContentID=11891) (January 2003)
(<http://www.ala.org/Template.cfm?Section=ifresolutions&Template=/ContentManagement/ContentDisplay.cfm&ContentID=11891>)

[State Chapter Resolutions](http://www.ala.org/Template.cfm?Section=stateifcinaction&Template=/ContentManagement/ContentDisplay.cfm&ContentID=25858)
(<http://www.ala.org/Template.cfm?Section=stateifcinaction&Template=/ContentManagement/ContentDisplay.cfm&ContentID=25858>)

[Resolution on Security and Access to Government Information](http://www.ala.org/Template.cfm?Section=issuesrelatedlinks&Template=/ContentManagement/ContentDisplay.cfm&ContentID=39337) (June 25, 2003)
(<http://www.ala.org/Template.cfm?Section=issuesrelatedlinks&Template=/ContentManagement/ContentDisplay.cfm&ContentID=39337>)

[Resolution Reaffirming the Principles of Intellectual Freedom in the Aftermath of the Terrorist Attacks](#) (January 23, 2002)
(<http://www.ala.org/Template.cfm?Section=ifresolutions&Template=/ContentManagement/ContentDisplay.cfm&ContentID=21668>)

[Resolution on the Terrorism Information Awareness Program](#) (June 25, 2003)
(<http://www.ala.org/Template.cfm?Section=issuesrelatedlinks&Template=/ContentManagement/ContentDisplay.cfm&ContentID=39339>)

[The USA Patriot Act in the Library](#) (<http://www.ala.org/ala/oif/ifissues/usapatriotactlibrary.htm>)

[Confidentiality and Coping with Law Enforcement Inquiries: Guidelines for the Library and its Staff](#) (last updated 2004)
(<http://www.ala.org/Template.cfm?Section=ifissues&Template=/ContentManagement/ContentDisplay.cfm&ContentID=21654>)

[FBI in Your Library](#) (<http://www.ala.org/oif/ifissues/fbiinyourlibrary>)

[Guidelines for Librarians on the USA PATRIOT Act: What to do before, during and after a "knock at the door?"](#) (January 19, 2002)
(<http://www.ala.org/ala/washoff/WOissues/civilliberties/theusapatriotact/patstep.pdf>)

[Surveillance in America](#) (<http://www.ala.org/oif/ifissues/surveillanceinamerica>)

[Terrorism Information and Prevention System \(TIPS\)](#) (<http://www.ala.org/oif/ifissues/tips>)

Statements of Other Library and Professional Associations

IFLA, "[The Glasgow Declaration on Libraries, Information Services and Intellectual Freedom](#)" (<http://www.ifla.org/faife/policy/iflastat/gldeclar-e.html>), (The Hague, Netherlands: IFLA, August 19, 2002).

IFLA, "[The IFLA Internet Manifesto](#)" (<http://www.ifla.org/III/misc/im-e.htm>), (The Hague, Netherlands: IFLA, August 23, 2002).

Canadian Library Association, [Citizenship Access to Information Data Banks - Right to Privacy](#) (<http://www.cla.ca/about/citizen.htm>), Approved by Executive Council ~ June, 1987.

[ACM Code of Ethics and Professional Conduct](#) (<http://www.acm.org/constitution/code.html>), Adopted by ACM Council 10/16/92.

[Software Engineering Code of Ethics and Professional Practice \(IEEE\)](#)
(<http://csciwww.etsu.edu/gotterbarn/SECEPP/page.asp?Name=Code>)

[Other Codes of Ethics for Computing and Information Sciences](#) (<http://www.emr.org/linksUCE.html>)

Privacy Policy Guidelines and Model Policy

[Guidelines for Developing a Library Privacy Policy](http://www.ala.org/oif/ifttoolkits/privacy/guidelines), HTML Version (links to WORD and PDF versions)
(<http://www.ala.org/oif/ifttoolkits/privacy/guidelines>)

[Model Privacy Policy](http://www.ala.org/oif/ifttoolkits/privacy/guidelines) (August 2003; rev. March 2005)
(<http://www.ala.org/oif/ifttoolkits/privacy/guidelines>)

Conducting a Privacy Audit

[Conducting a Privacy Audit](http://www.ala.org/ala/oif/ifttoolkits/toolkitsprivacy/guidelinesfordevelopingalibraryprivacypolicy/guidelinesprivacypolicy.htm) (August 2003)
(<http://www.ala.org/ala/oif/ifttoolkits/toolkitsprivacy/guidelinesfordevelopingalibraryprivacypolicy/guidelinesprivacypolicy.htm>)

Federal and State Privacy Laws and Policies; Freedom of Information Act; Court Orders

Federal Privacy Laws and Policies

[Privacy Act of 1974](http://www.epic.org/privacy/laws/privacy_act.html) (http://www.epic.org/privacy/laws/privacy_act.html)

- [Text of bill](http://www.epic.org/privacy/laws/privacy_act.html) (http://www.epic.org/privacy/laws/privacy_act.html)
- [Background and Updates](http://www.usdoj.gov/04foia/04_7_1.html) (http://www.usdoj.gov/04foia/04_7_1.html)
- [Consumer Guide](http://www.consumerprivacyguide.org/law/pa.shtml) (<http://www.consumerprivacyguide.org/law/pa.shtml>)

The Privacy Act of 1974, 5 U.S.C. § 552a (2000), was the first official Congressional statement about the importance of privacy, generally characterized as an omnibus "code of fair information practices" that attempts to regulate the collection, maintenance, use, and dissemination of personal information by federal executive branch agencies. The Act provides safeguards against an invasion of privacy through the misuse of records by Federal agencies and allows a citizen to learn how records are collected, maintained, used, and disseminated by the Federal Government. The act also permits an individual to gain access to most personal information maintained by Federal agencies and to seek amendment of any inaccurate, incomplete, untimely, or irrelevant information.

[Federal Educational Rights and Privacy Act \(FERPA\)](http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html)
(<http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html>)

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. The main focus of FERPA is to define who can access student records. FERPA grants parents the rights until the child turns 18 years old or attends a school beyond the high school level. The Act spells out the conditions that allow schools to release records without consent to certain designated parties. Title V, section 507 of the USA PATRIOT Act amended FERPA by creating a new exception to the privacy protections.

[Children's Online Privacy Protection Act \(COPPA\)](http://www.ala.org/ala/washoff/WOissues/civilliberties/coppa/coppalibrarians.htm)
(<http://www.ala.org/ala/washoff/WOissues/civilliberties/coppa/coppalibrarians.htm>)

The Children's Online Privacy Protection Act of 1998 (COPPA) (15 U.S.C. § 6501; 16 CFR 312) requires commercial online content providers who either have actual knowledge that they are dealing with a child 12 or under or who aim their content at children to obtain verifiable parental consent before they can collect, archive, use, or resell any personal information pertaining to that child. In addition, the Act requires commercial Web sites and online services covered by COPPA to place their information collection, use and disclosure practices prominently on their Web site. The law also mandates that site operators allow parents to review and delete information about their children collected by the site.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

(<http://www.cms.hhs.gov/hipaa/>)

- [HHS Privacy Rule](http://www.hhs.gov/ocr/hipaa/) (<http://www.hhs.gov/ocr/hipaa/>)
- [Health Privacy Project](http://www.healthprivacy.org/) (<http://www.healthprivacy.org/>)

The Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191, requires the adoption of national standards for electronic health care transactions and mandates the adoption of Federal privacy protections for individually identifiable health information. The new standards went into effect on April 14, 2003, outlining the responsibilities of health care providers and the rights of patients in providing access to individual health care information.

The Financial Modernization Act of 1999 (Gramm-Leach-Bliley Act)

(<http://www.ftc.gov/bcp/conline/pubs/buspubs/glbshort.htm>)

The Financial Modernization Act of 1999, Public Law 106-102, also known as the "Gramm-Leach-Bliley Act" or GLB Act, includes provisions to protect consumers' personal financial information held by financial institutions. There are three principal parts to the privacy requirements: the Financial Privacy Rule, Safeguards Rule and pretexting provisions. The Safeguards Rule requires all financial institutions to design, implement and maintain safeguards to protect customer information. The Rule applies not only to financial institutions that collect information from their own customers, but also to financial institutions -- such as credit reporting agencies -- that receive customer information from other financial institutions.

Student and Exchange Visitors Information System (SEVIS)

(<http://uscis.gov/graphics/shared/sevis/index.htm>)

The Student and Exchange Visitors Information System (SEVIS), administered by the Department of Homeland Security in partnership with the Department of State and the Department of Education, 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. Schools are now required to report a foreign student's failure to enroll or if students drop out of their programs. Certain requirements imposed by the Family Educational Rights and Privacy Act (FERPA) are waived and conditions for employment specified.

The Electronic Communications Privacy Act of 1986 (ECPA)

(<http://www.cpsr.org/issues/privacy/ecpa86>)

- [The Law](http://www.cpsr.org/issues/privacy/ecpa86) (<http://www.cpsr.org/issues/privacy/ecpa86>)
- [Analysis](http://www.cdt.org/security/000927hr5018.shtml) (<http://www.cdt.org/security/000927hr5018.shtml>)

The Electronic Communications Privacy Act (ECPA), Public Law 99-508, sets out the provisions for access, use, disclosure, interception and privacy protections of electronic communications. The law, which covers various forms of wire and electronic communications, prohibits unlawful access and certain disclosures of communication contents and prevents government entities from requiring disclosure of electronic communications from a provider without proper procedure. ECPA was amended by Sections 209- 212 and 216 of the USA PATRIOT ACT.

Federal Trade Commission's Consumer Protection, Privacy Oversight
(<http://www.ftc.gov/privacy/index.html>)

The Federal Trade Commission Consumer Protection Division, under Section 5 of the FTC Act, administers a privacy program in order to make sure that companies keep the promises they make to consumers about privacy and take precautions to secure consumers' personal information. The Commission has brought a number of cases to enforce the promises in privacy statements, including promises about the security of consumers' personal information.

Other Federal Privacy Legislation

Cable Communications Policy Act of 1984 (<http://www.consumerprivacyguide.org/law/ccpa.shtml>)

Cable Television Consumer Protection and Competition Act of 1992
(<http://www.lib.niu.edu/ipo/im940109.html>)

Communications Assistance to Law Enforcement Act (CALEA) of 1994
(<http://www.consumerprivacyguide.org/law/calea.shtml>)

Critical Infrastructure Information Protection (H.R. 5005-passed November 22, 2002; Public Law 107-296) (<http://www.foxnews.com/story/0,2933,133294,00.html>)

Digital Millennium Copyright Act of 1998 (<http://www.gseis.ucla.edu/iclp/dmca1.htm>)

Do-Not-Call Implementation Act of 2003 (http://www.mbaa.org/industry/docs/03/hr395_0213.pdf)

Driver's Privacy Protection Act of 1994 (<http://www.consumerprivacyguide.org/law/dppa.shtml>)

E-Government Act of 2002 (Requires Federal Agencies to conduct privacy impact assessments)
(<http://www.egov.vic.gov.au/International/TheAmericas/UnitedStates/E-government-Act-2002/e-government-act-2002.htm>)

The Enhanced Border Security and Visa Entry Reform Act of 2002
(<http://www.whitehouse.gov/news/releases/2002/05/20020514-4.html>)

The Fair Credit Reporting Act (1970) (<http://www.consumerprivacyguide.org/law/fcra.shtml>)

Foreign Intelligence Surveillance Act (FISA) (1978)
(http://straylight.law.cornell.edu/uscode/html/uscode50/usc_sup_01_50_10_36.html)

Homeland Security Act of 2002 (<http://www.whitehouse.gov/deptofhomeland/analysis/>)

[Illegal Immigration Reform and Immigrant Responsibility Act \(IIRIRA\) of 1996](http://www.immigration-usa.com/ina_96.html) (http://www.immigration-usa.com/ina_96.html)[Requires that educational institutions collect data for the [Student and Exchange Visitors Information System \(SEVIS\)](http://www.ice.gov/graphics/sevis/) (<http://www.ice.gov/graphics/sevis/>)]

[Privacy Protection Act of 1980](http://www.consumerprivacyguide.org/law/ppa.shtml) (<http://www.consumerprivacyguide.org/law/ppa.shtml>)

[Right to Financial Privacy Act \(1978\)](http://www.consumerprivacyguide.org/law/rfpa.shtml) (<http://www.consumerprivacyguide.org/law/rfpa.shtml>)

[Telecommunications Act of 1996](http://www.consumerprivacyguide.org/law/ta.shtml) (<http://www.consumerprivacyguide.org/law/ta.shtml>)

[Telephone Consumer Protection Act of 1991](http://www.consumerprivacyguide.org/law/tpa.shtml) (<http://www.consumerprivacyguide.org/law/tpa.shtml>)

[Video Privacy Protection Act of 1988](http://www.consumerprivacyguide.org/law/vppa.shtml) (<http://www.consumerprivacyguide.org/law/vppa.shtml>)

For information on privacy-related legislation, see:

[ALA Washington Office, Current Privacy Legislation](http://www.ala.org/ala/washoff/WOissues/civilliberties/privacy/privacyrelated.htm)
(<http://www.ala.org/ala/washoff/WOissues/civilliberties/privacy/privacyrelated.htm>)

[EPIC Bill Track: Tracking Privacy, Speech, and Cyber-Liberties Bills](http://www.epic.org/privacy/bill_track.html)
(http://www.epic.org/privacy/bill_track.html)

[Thomas Legislative Information on the Internet](http://thomas.loc.gov/cgi-bin/query/r?c107:@privacy) (<http://thomas.loc.gov/cgi-bin/query/r?c107:@privacy>)

[Pending Legislation Concerning the USA PATRIOT Act](http://www.ala.org/Template.cfm?Section=issuesrelatedlinks&Template=/ContentManagement/ContentDisplay.cfm&ContentID=49293)
(<http://www.ala.org/Template.cfm?Section=issuesrelatedlinks&Template=/ContentManagement/ContentDisplay.cfm&ContentID=49293>)

State Privacy Laws and Policies

Forty-eight states and the District of Columbia have library privacy and confidentiality laws. The language varies from state to state. These laws take two forms: affirmative protection of privacy for individuals who use libraries, and exemptions of libraries from open records or freedom of information laws. Libraries are advised to rely on existing laws to control behavior that involves public safety or criminal behavior.

[State Privacy Laws regarding Library Records](http://www.ala.org/oif/stateprivacylaws) (<http://www.ala.org/oif/stateprivacylaws>)

[Privacy Laws by State](http://www.epic.org/privacy/consumer/states.html) (<http://www.epic.org/privacy/consumer/states.html>)

FOIA and Libraries

[Open Records Requests Seeking Information Concerning Complaints About Patrons Accessing "Inappropriate" Material on Public Library Internet Terminals](http://www.ala.org/ala/oif/ifissues/issuesrelatedlinks/openrecordsrequests.htm) (May 12, 1999)
(<http://www.ala.org/ala/oif/ifissues/issuesrelatedlinks/openrecordsrequests.htm>)

Identify Types of Requests (Court Orders, etc.)

[Sample subpoena, trap/trace, preservation order, etc.](#)

<http://www.cybercrime.gov/s&sappendix2002.htm>

[Sample National Security Letters](#)

<http://www.ala.org/ala/oif/ifissues/nationalsecurityletter.pdf> (PDF)

[Sample FISA \(Section 215\) Order for Business Records](#)

<http://www.ala.org/ala/oif/ifissues/215formorder.pdf> (PDF)

[Sample Federal Search Warrants and Subpoenas](#)

<http://www.ala.org/ala/oif/ifissues/samplewarrants.pdf> (PDF)

Confidentiality and Coping with Law Enforcement Inquiries: Guidelines for the Library and its Staff

[Confidentiality and Coping with Law Enforcement Inquiries: Guidelines for the Library and its Staff](#)
(<http://www.ala.org/oif/ifissues/lawenforcementinquiries>)

Increased visits to libraries by law enforcement agents, including FBI agents and officers of state, county, and municipal police departments, are raising considerable concern among the public and the library community. These visits are not only a result of the increased [surveillance](http://www.ala.org/oif/ifissues/surveillanceinamerica) (<http://www.ala.org/oif/ifissues/surveillanceinamerica>) and investigation prompted by the events of September 11, 2001 and the subsequent passage of the [USA PATRIOT Act](http://www.ala.org/oif/ifissues/usapatriotact) (<http://www.ala.org/oif/ifissues/usapatriotact>), but also as a result of law enforcement officers investigating computer crimes, including e-mail threats and possible violations of the laws addressing online obscenity and child pornography. These guidelines, developed to assist libraries and library staff in dealing with law enforcement inquiries, rely upon the ALA's [Policy on Confidentiality of Library Records](http://www.ala.org/Template.cfm?Section=otherpolicies&Template=/ContentManagement/ContentDisplay.cfm&ContentID=13084) (<http://www.ala.org/Template.cfm?Section=otherpolicies&Template=/ContentManagement/ContentDisplay.cfm&ContentID=13084>), its [Policy Concerning Confidentiality of Personally Identifiable Information about Library Users](http://www.ala.org/Template.cfm?Section=otherpolicies&Template=/ContentManagement/ContentDisplay.cfm&ContentID=13087) (<http://www.ala.org/Template.cfm?Section=otherpolicies&Template=/ContentManagement/ContentDisplay.cfm&ContentID=13087>), and the [Code of Ethics](http://www.ala.org/oif/policies/codeofethics) (<http://www.ala.org/oif/policies/codeofethics>).

Privacy Tool Kit

<http://www.ala.org/ala/oif/iftoolkits/toolkitsprivacy/privacy.htm>

Guidelines for Developing a Library Privacy Policy

CONTENTS

I. Introduction

PII: Personally Identifiable Information

Privacy Policies and the Law

Privacy Policies and ALA

Your Library's Policy Should Incorporate Standard Privacy Principles

II. How to Draft a Library Privacy Policy

1. Notice & Openness
2. Choice & Consent
3. Access by Users
4. Data Integrity & Security
5. Enforcement & Redress

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

Academic Libraries

School Library Media Centers

Public Library Services to Minors

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

Checklist of Basic Questions about Privacy and Confidentiality

APPENDIX 1: Model Privacy Policy

APPENDIX 2: Conducting a Privacy Audit

APPENDIX 3: Sample Library Privacy and Confidentiality Policies

American Library Association

Guidelines for Developing a Library Privacy Policy

Prepared by the ALA Intellectual Freedom Committee

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 an individual's 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.

Selected Links:

- [American Library Association, Policy Concerning Confidentiality of Personally Identifiable Information about Library Users](http://www.ala.org/ala/oif/statementspols/statementspolicies.htm#privacy) (<http://www.ala.org/ala/oif/statementspols/statementspolicies.htm#privacy>)
- [Privacy Rights Clearinghouse, Privacy Survival Guide](http://www.privacyrights.org/fs/fs1-surv.htm) (<http://www.privacyrights.org/fs/fs1-surv.htm>)

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.

Selected Links:

- [First, Fourth, Fifth, Ninth, Tenth, and Fourteenth Amendments to the Constitution of the United States](http://www.ala.org/Template.cfm?Section=issuesrelatedlinks&Template=/ContentManagement/ContentDisplay.cfm&ContentID=25291) (<http://www.ala.org/Template.cfm?Section=issuesrelatedlinks&Template=/ContentManagement/ContentDisplay.cfm&ContentID=25291>)
- [Article Twelve of the Universal Declaration of Human Rights](http://www.un.org/Overview/rights.html) (<http://www.un.org/Overview/rights.html>)
- [Your Privacy Protection Under the Law](http://www.consumerprivacyguide.org/law/) (<http://www.consumerprivacyguide.org/law/>)
- [History of the Privacy Act of 1974](http://www.cavebear.com/nsf-dns/pa_history.htm) (http://www.cavebear.com/nsf-dns/pa_history.htm)
- [Privacy and the Courts](http://www.ala.org/Template.cfm?Section=issuesrelatedlinks&Template=/ContentManagement/ContentDisplay.cfm&ContentID=25293) (<http://www.ala.org/Template.cfm?Section=issuesrelatedlinks&Template=/ContentManagement/ContentDisplay.cfm&ContentID=25293>)
- [State Privacy Laws Regarding Library Records](http://www.ala.org/oif/stateprivacylaws) (<http://www.ala.org/oif/stateprivacylaws>)

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."

Selected Links:

- American Library Association, [Privacy Policies and Statements](http://www.ala.org/oif/ifissues/privacypolicies) (<http://www.ala.org/oif/ifissues/privacypolicies>)

- [American Library Association, Code of Ethics: History of the Code of Ethics](http://www.ala.org/ala/oif/statementspols/codeofethics/coehistory/Default2092.htm) (http://www.ala.org/ala/oif/statementspols/codeofethics/coehistory/Default2092.htm)
- [The American Library Association, Task Force on Privacy and Confidentiality in the Electronic Environment Final Report, 7 July 2000](http://www.ala.org/ala/lita/litaresources/taskforceonpriv/alataskforce.htm) (http://www.ala.org/ala/lita/litaresources/taskforceonpriv/alataskforce.htm)
- [American Library Association, Web Site Privacy Statement](http://www.ala.org/ala/home/privacystatement.htm) (http://www.ala.org/ala/home/privacystatement.htm) (April 3, 2003)

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.

Selected Links:

- United States Department of Health, Education and Welfare. [Records, Computers and the Rights of Citizens, Summary and Recommendations](http://aspe.hhs.gov/datacncl/1973privacy/Summary.htm) (http://aspe.hhs.gov/datacncl/1973privacy/Summary.htm) (1973)
- United States Federal Trade Commission, "[Chapter III: Fair Information Practice Principles](http://www.ftc.gov/reports/privacy3/fairinfo.htm)," Privacy Online: A Report to Congress (http://www.ftc.gov/reports/privacy3/fairinfo.htm) (June 1998)
- Organization for Economic Cooperation and Development (OECD), [Guidelines on the Protection of Privacy and Transborder Flows of Personal Data](http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html) (http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html) (Sept. 1980)
- International Federation of Library Associations (IFLA), "[The Glasgow Declaration on Libraries, Information Services and Intellectual Freedom](http://www.ifla.org/faife/policy/iflastat/gldeclar-e.html)" (http://www.ifla.org/faife/policy/iflastat/gldeclar-e.html)," (The Hague, Netherlands: IFLA, August 20, 2002)
- International Federation of Library Associations (IFLA), "[The IFLA Internet Manifesto](http://www.ifla.org/III/misc/im-e.htm)" (http://www.ifla.org/III/misc/im-e.htm)," (The Hague, Netherlands: IFLA, August 23, 2002)
- Canadian Library Association, "[Citizenship Access to Information Data Banks - Right to Privacy](http://www.cla.ca/about/citizen.htm)" (http://www.cla.ca/about/citizen.htm) (June, 1987)
- Privacy Rights Clearinghouse, [A Checklist of Responsible Information-Handling Practices](http://www.privacyrights.org/fs/fs12-ih2.htm) (http://www.privacyrights.org/fs/fs12-ih2.htm)
- Computer Professionals for Social Responsibility, [Electronic Privacy Principles](http://www.cpsr.org/issues/privacy/epp) (http://www.cpsr.org/issues/privacy/epp)

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:

- [Mill Valley Public Library Privacy Statement](http://millvalleylibrary.org/policypriv.html) (<http://millvalleylibrary.org/policypriv.html>)
- [Queens Borough Public Library](http://www.qbpl.org/about/policy/confidential.asp) (<http://www.qbpl.org/about/policy/confidential.asp>)
- [Florida State University Libraries](http://www.fsu.edu/library/explore/policies/privacy.shtml) (<http://www.fsu.edu/library/explore/policies/privacy.shtml>)

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:

- [Salem College Library](http://www.salem.edu/library/index.shtml) (<http://www.salem.edu/library/index.shtml>)
- [Brooklyn Public Library](http://www.brooklynpubliclibrary.org/) (<http://www.brooklynpubliclibrary.org/>)
- [Duke University Library](http://library.duke.edu/about/privacy.html) (<http://library.duke.edu/about/privacy.html>)
- [Santa Clara City Library](http://www.library.ci.santa-clara.ca.us/about-the-library/policies.html) (<http://www.library.ci.santa-clara.ca.us/about-the-library/policies.html>)

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.

Examples of Access Statements from Sample Library Privacy Policies:

- [Duke University](http://library.duke.edu/about/privacy.html) (<http://library.duke.edu/about/privacy.html>)
- [Salem College](http://www.salem.edu/privacy.html) (<http://www.salem.edu/privacy.html>)
- [John Carroll University](http://www.jcu.edu/library/statpol/jcuprivacypolicy.htm) (<http://www.jcu.edu/library/statpol/jcuprivacypolicy.htm>)
- [Seattle Public Library](http://www.spl.org/default.asp?pageID=help_siteindex) (http://www.spl.org/default.asp?pageID=help_siteindex)
- [Indian River Community College](http://www.universities.com/Schools/I/Indian_River_Community_College.asp) (http://www.universities.com/Schools/I/Indian_River_Community_College.asp)

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 library users access to their personal 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:

- ALA Task Force on Privacy and Confidentiality in the Electronic Environment. [Final Report](http://www.ala.org/ala/lita/litaresources/taskforceonpriv/alataskforce.htm) (http://www.ala.org/ala/lita/litaresources/taskforceonpriv/alataskforce.htm), 7 July 2000
- Berkeley Digital Library Sunsite, [Web Log Washing](http://sunsite.berkeley.edu/Web4Lib/RefCenter/logwashing.html) (http://sunsite.berkeley.edu/Web4Lib/RefCenter/logwashing.html)
- California Digital Library, [SOPAG Privacy Audit and Guidelines](http://libraries.universityofcalifornia.edu/sopag/privacytf/privacy_audit.html) (http://libraries.universityofcalifornia.edu/sopag/privacytf/privacy_audit.html)
- Center for Democracy and Technology, [Authentication Privacy Principles Working Group](http://www.cdt.org/privacy/authentication/030513interim.shtml) (http://www.cdt.org/privacy/authentication/030513interim.shtml)
- [CERT Tech Tips](http://www.cert.org/tech_tips/) (http://www.cert.org/tech_tips/)
- Cookie Central, [Frequently Asked Questions About Cookies](http://www.cookiecentral.com/faq/) (http://www.cookiecentral.com/faq/)
- Electronic Frontier Foundation, "[Privacy, Security, Crypto, & Surveillance](http://www.eff.org/Privacy/)" (http://www.eff.org/Privacy/) Archive
- The Electronic Privacy Information Center, [Cookie Page](http://www.epic.org/privacy/internet/cookies/) (http://www.epic.org/privacy/internet/cookies/)
- The Electronic Privacy Information Center, [International Data Retention Page](http://www.epic.org/privacy/intl/data_retention.html) (http://www.epic.org/privacy/intl/data_retention.html)
- International Coalition of Library Consortia, [Privacy Guidelines for Electronic Resources Vendors](http://www.library.yale.edu/consortia/2002privacyguidelines.html) (http://www.library.yale.edu/consortia/2002privacyguidelines.html)

- IEEE, [Security & Privacy Magazine](http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=8013) (http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=8013)
- Internet2, [The Shibboleth Project](http://shibboleth.internet2.edu/) (http://shibboleth.internet2.edu/)
- World Wide Web Consortium, [The World Wide Web Security FAQ: 8. Server Logs and Privacy](http://www.w3.org/Security/Faq/wwwsf3.html) (http://www.w3.org/Security/Faq/wwwsf3.html)

Examples of Retention Schedules from Sample Library Privacy Policies:

- [Spokane County Public Library](http://www.sclld.org/privacy.htm) (http://www.sclld.org/privacy.htm)
- [Colorado State University Library](http://lib.colostate.edu/) (http://lib.colostate.edu/)
- [Indiana University - Purdue Library](http://www.lib.ipfw.edu/410.0.html) (http://www.lib.ipfw.edu/410.0.html)
- [University of Michigan Library](http://www.lib.umich.edu/policies/privacy.html) (http://www.lib.umich.edu/policies/privacy.html)

Examples of Security Statements from Sample Library Privacy Policies:

- [Cleveland Heights-University Heights Public Library](http://www.heightslibrary.org/privacy.php) (http://www.heightslibrary.org/privacy.php)
- [Duke University Library](http://library.duke.edu/about/privacy.html) (http://library.duke.edu/about/privacy.html)
- [John Carroll University Library](http://www.jcu.edu/library/statpol/jcuprivacypolicy.htm) (http://www.jcu.edu/library/statpol/jcuprivacypolicy.htm)
- [Seattle Public Library](http://www.spl.org/default.asp?pageID=help_siteindex) (http://www.spl.org/default.asp?pageID=help_siteindex)
- [Syracuse University Library](http://libwww.syr.edu/policies/privacy.html) (http://libwww.syr.edu/policies/privacy.html)
- [University of Texas - Southwestern Library](http://www8.utsouthwestern.edu/utsw/home/facultyadministration/library/) (http://www8.utsouthwestern.edu/utsw/home/facultyadministration/library/)

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.

Selected Links:

- [ALA Office for Information Technology Policy, Top tips for Protecting Privacy Online](http://www.ala.org/ala/washoff/oitp/emailtutorials/privacya/15.htm) (http://www.ala.org/ala/washoff/oitp/emailtutorials/privacya/15.htm)
- [United States Federal Trade Commission, Privacy Tips](http://www.ftc.gov/bcp/online/pubs/alerts/privtipsalrt.htm) (http://www.ftc.gov/bcp/online/pubs/alerts/privtipsalrt.htm)

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](http://www.ala.org/ala/oif/ifissues/guidelineslibrary.pdf) (http://www.ala.org/ala/oif/ifissues/guidelineslibrary.pdf), April 2002
- [Suggested Procedures for Implementing Policy on Confidentiality of Library Records](http://www.ala.org/Template.cfm?Section=otherpolicies&Template=/ContentManagement/ContentDisplay.cfm&ContentID=20013) (http://www.ala.org/Template.cfm?Section=otherpolicies&Template=/ContentManagement/ContentDisplay.cfm&ContentID=20013), 1988
- [USA PATRIOT Act](http://www.ala.org/ala/oif/ifissues/usapatriotact.htm) (http://www.ala.org/ala/oif/ifissues/usapatriotact.htm), May 2003:
- [Guidelines for Librarians on the USA PATRIOT Act: What to do before, during and after a "knock at the door?"](http://www.ala.org/ala/washoff/WOissues/civilliberties/theusapatriotact/patstep.pdf) (http://www.ala.org/ala/washoff/WOissues/civilliberties/theusapatriotact/patstep.pdf), January 2002

To learn more about federal search and seizure guidelines, see:

- United States Department of Justice Criminal Division Computer Crime and Intellectual Property Section, [Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations](http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm) (http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm), July 2002

Examples of Disclosure/Court Order Statements from Sample Library Privacy Policies:

- [Fort Vancouver Regional Library District](http://66.96.75.5/aboutus/policies/confidentiality.htm) (http://66.96.75.5/aboutus/policies/confidentiality.htm)
- [Kansas City Public Library](http://www.kclibrary.org/) (http://www.kclibrary.org/)
- [Madison, WI, Public Library](http://www.madisonpubliclibrary.org/) (http://www.madisonpubliclibrary.org/)
- [Mansfield, OH](http://winslo.state.oh.us/publib/confid-mansfield.html) (http://winslo.state.oh.us/publib/confid-mansfield.html)
- [Queensboro Public Library](http://www.qbpl.org/about/policy/confidential.asp) (http://www.qbpl.org/about/policy/confidential.asp)
- [Carleton College](http://www.carleton.edu/campus/library/loan/circ.html#confidentiality) (http://www.carleton.edu/campus/library/loan/circ.html#confidentiality)
- [College of St. Catherine](http://www.stkate.edu/library/admin/privacy.html) (http://www.stkate.edu/library/admin/privacy.html)
- [Indiana University - Purdue](http://www.lib.ipfw.edu/410.0.html) (http://www.lib.ipfw.edu/410.0.html)
- [University of Michigan - Dearborn](http://libraryweb.umd.umich.edu/lib/privacy.html) (http://libraryweb.umd.umich.edu/lib/privacy.html)
- [Vanderbilt University](http://www.library.vanderbilt.edu/access/confidentiality.shtml) (http://www.library.vanderbilt.edu/access/confidentiality.shtml)

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:

- [Cause, Privacy and the Handling of Student Information in the Electronic Networked Environment of Colleges and Universities](http://www.educause.edu/ir/library/pdf/pub3102.pdf) (<http://www.educause.edu/ir/library/pdf/pub3102.pdf>), 1997
- American Library Association, [Intellectual Freedom Principles for Academic Libraries: An Interpretation of the Library Bill of Rights](http://www.ala.org/Template.cfm?Section=interpretations&Template=/ContentManagement/ContentDisplay.cfm&ContentID=76535) (<http://www.ala.org/Template.cfm?Section=interpretations&Template=/ContentManagement/ContentDisplay.cfm&ContentID=76535>)
- Barbara M. Jones, "[Academic Libraries and Intellectual Freedom](http://www.ala.org/ala/oif/iftoolkits/ifmanual/fifthedition/academiclibraries.htm)" (<http://www.ala.org/ala/oif/iftoolkits/ifmanual/fifthedition/academiclibraries.htm>)
- United States Department of Education, [Family Educational Rights and Privacy Act](http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html) (<http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html> ; FERPA)
- United States Department of Education, [Protecting the Privacy of Student Records, Guidelines for Education Agencies](http://nces.ed.gov/pubs97/97527.pdf) (<http://nces.ed.gov/pubs97/97527.pdf>)
- United States Department of Homeland Security, [SEVP: Student and Exchange Visitor Program](http://www.ice.gov/graphics/sevis/index.htm) (<http://www.ice.gov/graphics/sevis/index.htm>)
- Virginia Rezmierski and Nathaniel St. Clair, II, [Identifying Where Technology Logging and Monitoring for Increased Security End and Violations of Personal Privacy and Student Records Begin: Final Report NS-LAMP Project](#), Washington, DC: American Association of Collegiate Registrars and Admissions Officers, 2001

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/ala/aasl/aaslproftools/positionstatements/aaslpositionstatementconfidentiality.htm)
(http://www.ala.org/ala/aasl/aaslproftools/positionstatements/aaslpositionstatementconfidentiality.htm)
- [Association for Library Service to Children, Internet Privacy and Safety Information for Parents](http://www.ala.org/ala/alsc/alscresources/forlibrarians/internettech/internetprivacysafety.htm)
(http://www.ala.org/ala/alsc/alscresources/forlibrarians/internettech/internetprivacysafety.htm)
- [American Library Association, Office for Information Technology Policy, COPPA for Parents](http://www.ala.org/ala/washoff/WOissues/civilliberties/coppa/coppaparents.htm)
(http://www.ala.org/ala/washoff/WOissues/civilliberties/coppa/coppaparents.htm)
- [Examples of COPPA Situations](http://www.ala.org/ala/washoff/WOissues/civilliberties/coppa/coppaexamples.htm)
(http://www.ala.org/ala/washoff/WOissues/civilliberties/coppa/coppaexamples.htm)
- [Selected Testimonies to the Child Online Protection Act Commission](http://www.ala.org/Template.cfm?Section=issuesrelatedlinks&Template=/ContentManagement/ContentDisplay.cfm&ContentID=28197)
(http://www.ala.org/Template.cfm?Section=issuesrelatedlinks&Template=/ContentManagement/ContentDisplay.cfm&ContentID=28197)
- [United States Department of Education, Family Policy Compliance Office Web Site](http://www.ed.gov/policy/gen/guid/fpco/index.html)
(http://www.ed.gov/policy/gen/guid/fpco/index.html)
- [Legal Information Institute, Family educational and privacy rights from the US Code](http://www4.law.cornell.edu/uscode/20/1232g.html)
(http://www4.law.cornell.edu/uscode/20/1232g.html)

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.

Selected links:

- YALSA, [Web Site](http://www.ala.org/ala/yalsa/yalsa.htm) (<http://www.ala.org/ala/yalsa/yalsa.htm>)
- [Especially for Children and Their Parents—Privacy](http://www.ala.org/ala/oif/foryoungpeople/childrenparents/especiallychildren.htm#privacy) (<http://www.ala.org/ala/oif/foryoungpeople/childrenparents/especiallychildren.htm#privacy>)
- [Minors' Rights to Receive Information Under the First Amendment](http://www.ala.org/Template.cfm?Section=issuesrelatedlinks&Template=/ContentManagement/ContentDisplay.cfm&ContentID=28210) (<http://www.ala.org/Template.cfm?Section=issuesrelatedlinks&Template=/ContentManagement/ContentDisplay.cfm&ContentID=28210>)
- [COPPA for Parents](http://www.ala.org/ala/washoff/WOissues/civilliberties/coppa/coppaparents.htm) (<http://www.ala.org/ala/washoff/WOissues/civilliberties/coppa/coppaparents.htm>)

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?

American Library Association 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 handling 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.

American Library Association

Guidelines for Developing a Library Privacy Policy

Appendix 2

Conducting a Privacy Audit

August 2003

Definition and Purpose: A privacy audit is a technique for assuring that an organization's goals and promises of privacy and confidentiality are supported by its practices, thereby protecting confidential information from abuse and the organization from liability and public relations problems. An audit ensures that information processing procedures meet privacy requirements by examining how information about library users and employees is collected, stored, shared, used and destroyed. Privacy auditing is a process, not a one-time solution, as services, data needs, and technology change. A designated Privacy Officer may lead the audit, but all stakeholders and aspects of privacy need to be represented, from information technology to public relations. The audit process needs to be capable of dealing with the full extent of the information system. When a library is part of a larger organization that is conducting a privacy audit, specific library issues and needs must be included.

The audit process begins by evaluating the organization's existing policies and procedures for legality and consistency with the organization's mission and image. When policies have been reviewed (or established), the data collected can be categorized according to the degree of security necessary. The audit assesses the sensitivity, security risks, and public perceptions of the information the organization collects. The audit examines the necessity for each type of data, how it is collected, and what notice and options are provided to the individuals identified by the information. Mapping how data flows through the organization for access, storage, and disposal can reveal security needs, both electronic and physical. The audit process itself must be managed so that it does not increase risks and its recommendations must be addressed quickly once risks are revealed.

A privacy audit provides a library with an opportunity to examine:

- How privacy matters are handled at all levels.
- The flow and storage of data.
- The role data plays within the organization.
- Staff training about privacy matters.
- Existing and needed privacy policies.

What to Audit for Personally Identifiable Information:

(Based on: Karen Coyle, "Make Sure You Are Privacy Literate" 10/1/2002, Library Journal, v.127, #16: <http://libraryjournal.reviewsnews.com/index.asp?layout=article&articleid=CA245045> —reprinted with permission)

- Patron Records
- Circulation transaction logs
- Overdue and billing records
- Document delivery and interlibrary loan transactions
- Records of access to electronic reserves
- Records that support personalized services
- Search histories saved beyond a session
- Saved searches and sets
- SDI profiles
- Files/logs of previous electronic reference queries and answers
- System logs
- OPAC search logs
- Library Web server logs, including proxy servers
- Mail message files
- Mail server logs
- Public workstations
- Browser caches, including history files
- Cookies and certificates
- Browser bookmarks
- Paper sign-up sheets
- Licensed services
- Shared computer systems and servers
- Back up tapes stored locally and off site
- Remote Web sites, including content providers, outsourced Web hosting, proxy servers, etc.
- Personalization profiles and other service offers for personal information
- Usage statistics.
- Signed Internet/e-mail acceptable use agreements

Selected Sources:

- California Digital Library, [SOPAG Privacy Audit and Guidelines](http://libraries.universityofcalifornia.edu/sopag/privacytf/privacy_audit.html) (http://libraries.universityofcalifornia.edu/sopag/privacytf/privacy_audit.html)
- Karen Coyle, "[Make Sure You Are Privacy Literate](http://libraryjournal.reviewsnews.com/index.asp?layout=articlePrint&articleID=CA245045)" (http://libraryjournal.reviewsnews.com/index.asp?layout=articlePrint&articleID=CA245045)," Library Journal, v. 127, #16, October 1, 2002 (last accessed June 6, 2003).
- Karen Coyle, [Privacy and Library Systems Before & After 9/11](http://www.kcoyle.net/stbarb.html) (http://www.kcoyle.net/stbarb.html), 2002.
- Keith P. Enright, [Privacy Audit Checklist](http://cyber.law.harvard.edu/clinical/privacyaudit.html) (http://cyber.law.harvard.edu/clinical/privacyaudit.html), 2001.
- David H. Flaherty, [How To Do A Privacy And Freedom Of Information Act Site Visit](http://www.pco.org.hk/english/infocentre/files/flaherty-2.doc) (http://www.pco.org.hk/english/infocentre/files/flaherty-2.doc), 2001.
- Pamela Jerskey, Ivy Dodge, and Sanford Sherizen, [The Privacy Audit: a Primer](http://www2.bc.edu/~jerskey/privacy.htm) (http://www2.bc.edu/~jerskey/privacy.htm), 1998.
- Texas Department of Information Resources, [Privacy Issues Involved in Electronic Government](http://www.dir.state.tx.us/taskforce/report/privacy.htm) (http://www.dir.state.tx.us/taskforce/report/privacy.htm), 2000.

American Library Association

Guidelines for Developing a Library Privacy Policy

Appendix 3

Sample Library Privacy and Confidentiality Policies

August 2003

(Add your library's newly revised privacy policy by contacting Don Wood, ALA Office for Intellectual Freedom, dwood@ala.org. Be sure to include the URL.)

Public Libraries

[Brooklyn Public Library](http://www.brooklynpubliclibrary.org/) (<http://www.brooklynpubliclibrary.org/>)

[Cleveland Heights-University Heights Public Library](http://www.heightslibrary.org/privacy.php) (<http://www.heightslibrary.org/privacy.php>)

[Fort Vancouver Regional Library District](http://66.96.75.5/aboutus/policies/confidentiality.htm) (<http://66.96.75.5/aboutus/policies/confidentiality.htm>)

[Kansas City Public Library](http://www.kclibrary.org/) (<http://www.kclibrary.org/>)

[Madison, WI, Public Library](http://www.madisonpubliclibrary.org/) (<http://www.madisonpubliclibrary.org/>)

[Mansfield, OH](http://winslo.state.oh.us/publib/confid-mansfield.html) (<http://winslo.state.oh.us/publib/confid-mansfield.html>)

[Mill County Public Library](http://millvalleylibrary.org/policynet.html) (<http://millvalleylibrary.org/policynet.html>)

[Minneapolis Public Library](http://www.mplib.org/) (<http://www.mplib.org/>)

[Multnomah County's statement](http://www.multcolib.org/news/patriotact.html) (<http://www.multcolib.org/news/patriotact.html>)

[New York Public Library](http://www.nypl.org/) (<http://www.nypl.org/>)

[SIBL e-Reference](http://www.nypl.org/research/sibl/eforms/eref/privacy.htm) (<http://www.nypl.org/research/sibl/eforms/eref/privacy.htm>)

[Paulding Co. Ohio USA PATRIOT Act policy](#)

[Queensboro Public Library](http://www.pauldingcountylibrary.org/patriotactpolicy.htm) (<http://www.pauldingcountylibrary.org/patriotactpolicy.htm>)

[Santa Clara City Public Library](http://www.library.ci.santa-clara.ca.us/about-the-library/policies.html) (<http://www.library.ci.santa-clara.ca.us/about-the-library/policies.html>)

[Santa Cruz Public Library](http://www.santacruzpl.org/service/patdata.shtml) (<http://www.santacruzpl.org/service/patdata.shtml>)

[Seattle Public Library](http://www.spl.org/default.asp?pageID=help_siteindex) (http://www.spl.org/default.asp?pageID=help_siteindex)

[Spokane County](http://www.sclد.org/privacy.htm) (<http://www.sclد.org/privacy.htm>)

Academic and Research Libraries

[Amherst College](http://www.amherst.edu/library/info/privacy.html) (<http://www.amherst.edu/library/info/privacy.html>)

[California Digital Library](http://libraries.universityofcalifornia.edu/sopag/privacytf/) (<http://libraries.universityofcalifornia.edu/sopag/privacytf/>)

[Carleton College](http://www.carleton.edu/campus/library/loan/circ.html#confidentiality) (<http://www.carleton.edu/campus/library/loan/circ.html#confidentiality>)

[College of Charleston](http://www.cofc.edu/~library/admin/pol15.html) (<http://www.cofc.edu/~library/admin/pol15.html>)

[College of St. Catherine](http://www.stkate.edu/library/admin/privacy.html) (<http://www.stkate.edu/library/admin/privacy.html>)

[Colorado State University](http://welcome.colostate.edu/) (<http://welcome.colostate.edu/>)

[Drake University](http://www.drake.edu/) (<http://www.drake.edu/>)

[Duke University](http://library.duke.edu/about/privacy.html) (<http://library.duke.edu/about/privacy.html>)

[Florida State University](http://www.fsu.edu/library/explore/policies/privacy.shtml) (<http://www.fsu.edu/library/explore/policies/privacy.shtml>)

[Illinois Institute of Technology](http://www.gl.iit.edu/policy/privacy.htm) (<http://www.gl.iit.edu/policy/privacy.htm>)

[Indian River Community College](http://www.universities.com/Schools/I/Indian_River_Community_College.asp)
(http://www.universities.com/Schools/I/Indian_River_Community_College.asp)

[Indiana University - Purdue](http://www.lib.ipfw.edu/410.0.html) (<http://www.lib.ipfw.edu/410.0.html>)

[Jimmy Carter Library Web Site Privacy Statement](http://www.jimmycarterlibrary.org/privacy.phtml) (<http://www.jimmycarterlibrary.org/privacy.phtml>)

[John Carroll University](http://www.jcu.edu/library/statpol/jcuprivacypolicy.htm) (<http://www.jcu.edu/library/statpol/jcuprivacypolicy.htm>)

[Lake Michigan College](http://www.lakemichigancollege.edu/) (<http://www.lakemichigancollege.edu/>)

[Salem College](http://www.salem.edu/privacy.html) (<http://www.salem.edu/privacy.html>)

[Syracuse University](http://libwww.syr.edu/policies/privacy.html) (<http://libwww.syr.edu/policies/privacy.html>)

[University of Michigan](http://www.lib.umich.edu/policies/privacy.html) (<http://www.lib.umich.edu/policies/privacy.html>)

[University of Michigan - Dearborn](http://libraryweb.umd.umich.edu/lib/privacy.html) (<http://libraryweb.umd.umich.edu/lib/privacy.html>)

[University of Texas - Southwestern Medical Center](http://www8.utsouthwestern.edu/utsw/home/facultyadministration/library/)
(<http://www8.utsouthwestern.edu/utsw/home/facultyadministration/library/>)

[Vanderbilt University](http://www.library.vanderbilt.edu/access/confidentiality.shtml) (<http://www.library.vanderbilt.edu/access/confidentiality.shtml>)

School Libraries

Many school districts have policies on the confidentiality of library records, Internet use that include privacy statements, e-mail, student use agreements, and other statements that outline guidelines for ensuring privacy and confidentiality of personally identifiable information of students and teachers.

Library Associations

[American Library Association](http://www.ala.org/) (http://www.ala.org/)

[American Library Association Privacy Statement](http://www.ala.org/ala/home/privacystatement.htm) (http://www.ala.org/ala/home/privacystatement.htm), April 3, 2003.

[California Library Association](http://www.cla-net.org/privacy.php) (http://www.cla-net.org/privacy.php)

[Illinois Library Association](http://www.ila.org/advocacy/privacy.htm) (http://www.ila.org/advocacy/privacy.htm)

Adopted by the ALA Intellectual Freedom Committee, August 2003; revised March 5, 2004.

The ALA Intellectual Freedom Committee welcomes feedback from librarians utilizing these guidelines to develop and revise their library privacy policies. Please send comments to: Don Wood, ALA Office for Intellectual Freedom, dwood@ala.org.

Privacy Tool Kit

<http://www.ala.org/ala/oif/iftoolkits/toolkitsprivacy/privacy.htm>

PRIVACY PROCEDURES

Responsibilities of Governing Bodies/Policy Makers

- Keep informed about issues relating to library patron and user privacy and confidentiality
- Be aware of applicable federal, state and local laws and regulations
- Adopt appropriate policies
- Provide the library administration with sufficient resources to develop procedures and provide staff training in support of policies
- Understand and respect the library's organization and administrative hierarchy
- Understand the library's plan for routine and crisis communication
- Be knowledgeable about techniques for dealing with the media
- Be aware of the library's relationship to governmental agencies and officials (elected and appointed) and to other organizations

Responsibilities of Administrators

- Keep informed about issues relating to library patron and user privacy and confidentiality
- Be aware of applicable federal, state and local laws and regulations
- Inform and educate policy makers about relevant professional, ethical and legal issues
- Recommend privacy and confidentiality policies to policy makers:
 - Ensure that knowledgeable legal counsel is consulted
 - Include ALA and other relevant documents, laws and regulations;
- Make sure that all contracts with ILS (integrated library system) and other vendors are consistent and compliant with the library's policies
- Conduct privacy audits
 - Review and evaluate current practices and procedures
- Develop guidelines and procedures in support of policies:
 - Define patron privacy and confidentiality
 - Include relevant library policies
 - Identify the type and nature of all records and files that contain library patron and user personally identifiable information
 - Establish a schedule for the retention of records and files containing library patron and user personally identifiable information
 - Create a chart of the library's organizational hierarchy, indicating:
 - Chain of command
 - Staff members authorized to respond to requests for patron or user personally identifiable information
 - Define and describe the type and nature of requests for personally identifiable information:
 - Informal
 - Define the circumstances under which, the manner of and extent to which, patron and user personally identifiable information may be disclosed in person, over the phone or electronically
 - Law enforcement
 - Detail the specific steps staff should follow in responding to investigatory requests for patron and user personally identifiable information from:
 - Local and state agencies
 - Federal agencies

- Write a ready-reference card with a clear and concise description of the library's privacy policies
 - Make available in all departments and public service areas
- Be authorized to accept and comply with all investigatory requests
- Designate a library staff member to serve as the Library Privacy Officer who will:
 - Keep abreast of news and information about privacy issues
 - Train all library staff on privacy and confidentiality issues, policies and procedures:
 - Specify what, how, when and which staff may respond to public, media or law enforcement requests for library patron and user personally identifiable information
 - Examine staff practices and procedures on a regular basis for compliance with policies
 - Evaluate training methods and effectiveness
- Develop a routine and crisis communication plan:
 - Prepare an organizational chart/hierarchy of whom staff should contact
 - Maintain current contact information
- Designate a library spokesperson
- Provide media training for policy-makers and key staff
- Educate the public about issues of library privacy and confidentiality and the library's policies, practices and procedures to protect library patron and user personally identifiable information
- Maintain contact with local, regional and national affinity organizations
- Forge alliances with community groups

Responsibilities of Supervisors

- Reinforce training to ensure that all staff have a basic understanding of the library's policies, practices and procedures
- Monitor staff for compliance with library practices and procedures in their daily activities
- Report flaws or failures of training or procedures to the Privacy Officer
- Be prepared to discuss privacy and confidentiality policies, practices and procedures with library patrons and users

Staff Responsibilities

- Understand and follow library practices and procedures:
 - Apply equally to all library patrons and users regardless of age, origin, background or views
 - Maintain privacy and confidentiality when assisting library patrons and users
- Discuss matters of library patron and user personally identifiable information with other staff only when necessary for operational purposes:
 - Conduct discussions in non-public areas
- Refrain from discussing matters of library patron and user personally identifiable information with friends, family or members of the public
- Refer requests by the public, the media or law enforcement for access to, or view of, non-public computers, files or records to a library administrator
- Direct all requests from law enforcement or government officials for library patron and user personally identifiable information to a library administrator
- Keep confidential the source of any request or the nature of the information requested with staff, family, friends or members of the public

Privacy Communication

[Crisis Communication](#)

[Messages/Talking Points](#)

[Tips for Ensuring Privacy](#)

[Legislative Advocacy](#)

Privacy Tool Kit

<http://www.ala.org/ala/oif/iftoolkits/toolkitsprivacy/privacy.htm>

Crisis Communication with the Media

[Adapted from *Principles of Crisis Communication: After 9/11* (http://www.ala.org/Source/crisis_communicationjune.ppt), prepared for ALA by Brian Specht (ALA Annual Conference 2002); and *Communicating in a Crisis*, prepared by Nancy Kranich (1-10-05)]

A crisis is a difficult period of actual or perceived damage to an institution, unit, or individual, triggered by a sudden event or a rapidly developing problem. A crisis may affect safety or security, financial stability, reputation or the general ability to conduct business.

Crisis communication pertains to the exchange of information among the library administration, its governing body, and staff as well as between the library and law enforcement officials, the media, governmental agencies and the general public. A crisis communication plan addresses both preparedness and incident response.

Before a Crisis Occurs

- Develop a Crisis Communication Plan.
- Create a Crisis Management Team.
- Create a Crisis Communication Team, including spokespeople.

Developing the Crisis Communication Plan

- Prepare audience lists (media, stakeholders, friends).
- Reach out to media regularly and maintain key relationships.
- Have your policy guidelines and institutional facts updated and available.
- Reference the library's policies, relevant ALA documents and applicable federal, state and local laws.
- Evaluate all practices for handling print and electronic records and files, the library's physical plant, and the level of staff awareness of privacy and confidentiality of patron and user-identifiable information.
- Assess potential crises and draft talking points/statements.
- Seek opportunities to neutralize potential flash points.
- Monitor news for potential emerging problems.
- Be prepared to respond readily and accurately to a 24-hour global media - your response mechanism should be equal to the speed of the media.
- Conduct drills to stay sharp.

Organize Your Teams

- Develop and maintain a comprehensive contact list for teams (24 hour contact information).
- Establish a notification system.
- Clarify lines of responsibility, authority, and communication channels.

- Determine who should handle all inquiries in the absence of the Director, the Privacy Officer (staff member authorized to accept or comply with investigatory requests) or Administrator (most senior member of the organization on duty).
- Designate who will handle communications with the staff, media, public and other government agencies.
- Meet periodically to discuss potential threats and develop strategies.
- Train all full and part-time paid and volunteer employees on the library's policies, procedures and crisis communication plan.

Crisis Management Team:

- Library leader
- Key librarians and staff
- Trustees representative
- Volunteers representative
- Communications (see below)
- Legal counsel
- Make sure you are prepared to quickly reach out to key friends and allies of the library

Crisis Communication Team:

- responsible for all aspects of communication, including information gathering, media contacts, and public relations

Spokespeople:

- Designate a limited number of spokespeople.
- Select spokespeople who have credibility with their corresponding audience(s).
- Use most senior leader to take overall accountability.
- Training is vital - even a quick on the spot "mock interview" can be very helpful.

Communications Goals in a Crisis

- Contribute to ending the crisis
- Protect your library's reputation
- Reduce tension
- Demonstrate commitment to values
- Communicate promptly and continuously to maintain control of flow of information

Ground Rules: The Three "Cs"

- Candor: be honest, take necessary responsibility, and don't set unreasonable expectations.
- Concern: concern for health and safety needs to be foremost in responding. Show some controlled emotion and empathy (but don't overdo it!).
- Courage: Don't hide from the issue. A leader is not afraid to stand up, take responsibility, and get at the source of a problem.

Crisis Communication Team-Internal Preparations

- Consider, above all other factors, the health/safety of visitors, employees, public and community.
- Gather all facts as rapidly as possible.
- Immediately notify—and maintain contact with—appropriate local authorities (Police, Fire, etc.).
- Have someone with a legal perspective involved.
- Develop talking points to answer predictable questions.
- Maintain records of all proceedings.
- Encourage candid discussion of solutions.
- Communicate quickly and fully with one another.
- Monitor events and adapt as necessary.
- Lead and facilitate investigation.
- Don't be afraid to say "I don't know."

Crisis Communication Team - External Issues

- Understand the direct correlation between crises and brand management.
- Conduct a risk/benefit analysis to determine whether to go public, keeping in mind that those institutions that were forthcoming in a crisis (e.g., Tylenol case) fared better than those that were reticent (e.g., Firestone tire recall).
- Centralize incoming calls to appropriate spokespeople.
- Respond as quickly as possible to media calls—but don't panic and don't compromise accuracy.
- Make announcements promptly, unless special circumstances exist.
- Tell good stories so when bad news comes along you are given the benefit of the doubt.
- Do not fight with journalists even though you are under a lot of pressure.
- If a crisis is sustained, assign people to serve in shifts.
- Keep log of responses to journalists.
- Get the bad news out fast and get it over with.
- Apologize: accept responsibility when you are at fault - your credibility is on the line.
- Never lie.
- Monitor news reports so you can quell rumors and correct inaccuracies.
- Provide information that gives public alternatives.
- Communicate with each audience as directly as possible.

The Internet in a Crisis

- **Your Web site**
- Add crisis news promptly.
- Consider a "dark Web site" to activate quickly in extreme situations.

Internet

- Monitor news reports, specific sites and chat rooms.
- Monitor incoming e-mail closely.

Some Questions to Expect

- What caused the incident?
- What is the library procedure to handle such an incident?

- Will there be an investigation?
- What is being done to mitigate the risk?
- Has this happened before? If so, when?
- What is the library policy on this matter?

Developing Your Messages

- Clarify your objective.
- Organize your facts.
- Anticipate your toughest questions.
- Know what you want, and don't want, to say.
- Stay focused on 2-3 Key Messages (facts, concern, commitment, action).
- Use anecdotes, examples and illustrations.

When Risk and Fear are Issues

- Listen. Don't be compelled to constantly speak.
- When you do, speak clearly and with concern.
- Avoid unreasonable comparisons and statistics.
- Tell what you know, what you don't know.
- Whenever possible talk about actions.

Identify Your Audiences

- Library Users/General Public
- Employees
- Community
- Government/Law Enforcement
- Media
- Any others
- Use appropriate tools to communicate with each audience; be proactive when communicating with public and use outlets you control, like your web site.

After the Crisis

- Debrief everyone involved for lessons learned
- Review actions taken and look for missteps to be corrected
- Praise what was done well
- Document actions and keep on file for future reference

Crisis Rules to Live By

- Be part of the solution (especially if you were part of the problem).
 - Honesty is STILL the best policy.
 - And, be prepared. It can make ALL the difference.
-

See also: *The Library's Crisis Communications Planner: A PR Guide for Handling Every Emergency* / Jan Thenell. Chicago: ALA Editions, 2004. ISBN: 0-8389-0870-5.

Privacy Tool Kit

<http://www.ala.org/ala/oif/iftoolkits/toolkitsprivacy/privacy.htm>

Library Privacy Key Messages and Tough Questions

Key Messages

- [Privacy is essential to the exercise of free speech, free thought and free association](http://www.ala.org/ala/oif/statementspols/statementspolicies.htm#privacy) (<http://www.ala.org/ala/oif/statementspols/statementspolicies.htm#privacy>).
- Libraries are a cornerstone of democracy and help ensure Americans are able to read, research, and think freely.
- Forty-eight states and the District of Columbia have [statutes declaring library records as confidential documents](http://www.ala.org/ala/oif/stateprivacylaws) (<http://www.ala.org/ala/oif/stateprivacylaws>). The two remaining states, Hawaii and Kentucky, have opinions issued by their attorneys general finding library records to be confidential documents
- Librarians have always cooperated with law enforcement within the framework of state confidentiality laws and statements on the books in every state.
- Librarians have a responsibility to protect the privacy of our patrons while responding to legitimate national security concerns.

Tough Questions About Library Privacy

Why do libraries protect the confidentiality of library reading records?

- Forty-eight states and the District of Columbia have statutes declaring library records as confidential documents. The two remaining states, Hawaii and Kentucky, have opinions issued by their attorneys general finding library records to be confidential documents.
- States created these confidentiality laws to protect the privacy and freedoms Americans hold dear. These laws provide a clear framework for responding to national security concerns while safeguarding against random searches, fishing expeditions or invasions of privacy.
- Laws protecting the confidentiality of library records help to assure that no person comes under suspicion simply because he or she reads a disapproved book, or does research into a disapproved topic. Reading about chemistry does not make a person a terrorist bomber, nor should reading about childbirth and parenting place you under suspicion for abandoning an infant.
- Librarians maintain records to ensure the efficient operation of the library, not to review or document individuals' reading habits. Libraries do not keep or maintain print or electronic records as a means of law enforcement.
- It is standard practice that libraries do not create nor maintain unnecessary records. In fact, this is such a common practice that standard circulation software used by libraries automatically erases a circulation record after the materials are returned to the library.

What is ALA's position on the confidentiality of library records?

- The ALA encourages libraries to put in place procedures for working with law enforcement officers when a subpoena or other legal order for records is made. Libraries will cooperate expeditiously with law enforcement within the framework of the law.

- The ALA recommends that libraries seek legal counsel to ensure proper handling of search requests. The intersection of federal and state privacy laws is a complicated matter and needs to be decided on a case-by-case basis.
- If librarians do not follow state confidentiality laws and legal procedures, they run the risk of actually hurting ongoing police investigations. The American judicial system provides the mechanism for seeking release of confidential records: the issuance of a court order, showing probable cause based on specific facts and in proper form.

Why does the American Library Association oppose certain provisions of the USA PATRIOT Act?

- The American Library Association is concerned about the provisions of the [USA PATRIOT Act](http://www.ala.org/oif/ifissues/usapatriotact) (<http://www.ala.org/oif/ifissues/usapatriotact>) that allow the FBI to seek information on Americans' reading habits, as if it were possible to determine what someone might do based on what he or she has read.
- Librarians, like all Americans, are concerned about terrorism and the safety of our families and friends. But, the threat of terrorism must not be used as an excuse to intrude on our basic constitutional rights. We can fight terrorism, but we can do it at the same time as we protect the civil liberties that have made our country great.
- Section 215 of the Patriot Act greatly expanded the FBI's ability to get records from all businesses, including libraries and booksellers, without meeting the traditional standard needed to get a search warrant in the United States.
- Individual libraries may not be at liberty to discuss the specifics of any legal search, since a gag order accompanies a search warrant or subpoena issued under the USA PATRIOT Act.
- The American Library Association encourages all librarians, library administrators, and library advocates to educate their communities about the process for compliance with the USA PATRIOT Act and other related measures and about the dangers to individual privacy and the confidentiality of library records resulting from those measures.
- The ALA supports amendments to the USA PATRIOT Act and active oversight of the implementation of the USA PATRIOT Act.

What are ALA's concerns about the Attorney General's FBI guidelines revised in 2002?

- Under the revised [Attorney General's Guidelines on General Crimes, Racketeering and Terrorism](http://www.usdoj.gov/olp/generalcrimes2.pdf) (<http://www.usdoj.gov/olp/generalcrimes2.pdf>), which are separate from the USA PATRIOT, the FBI enjoys expanded powers to investigate terrorism and clandestine espionage by being able to do sweeping surveillance of groups of library patrons, not just related to investigations focused on one subject.
- By conducting sweeping investigations, law enforcement has access to everyone and anyone's records. Even when seeking information about a particular suspect, circulation records and databases may be obtained by law enforcement about an entire group of library users.
- While as Americans we also are concerned about our nation's security, librarians will continue to fight for their patrons' First Amendment right to read and receive information without government interference.

What was the FBI Library Awareness Program and how did the library community respond?

- Many librarians and library users are still around who recall the [FBI Library Awareness Program](http://www.ala.org/oif/ifissues/fbiinyourlibrary) (<http://www.ala.org/oif/ifissues/fbiinyourlibrary>) of the 1970s and 80s, when the FBI inappropriately attempted to monitor patrons' reading habits and obtain personal information about library users. The library community is anxious that this not be repeated.
- Through this program, which went on for decades, the FBI sought information on the reading habits of people from "hostile foreign countries," as well as U.S. citizens who held unpopular political views.

Privacy Tool Kit

<http://www.ala.org/ala/oif/ifttoolkits/toolkitsprivacy/privacy.htm>

Tips for Ensuring Privacy

Tips for Ensuring Privacy

- You should know that there are many laws protecting your privacy. These can be found at the federal level in the Constitution and in numerous federal laws, at the state level in state constitutions and other legislation, and even at the local level in municipal ordinances.
- Libraries should have an easily accessible privacy policy that tells patrons about the type of records kept by the library, reviews the laws that protect library records for their jurisdiction, discusses conditions for releasing information to third parties (like law enforcement), and lists the security measures for protecting online privacy while using library Internet services.

Online privacy for everyone:

- Don't select passwords that are easy to figure out, like your pet's name. Instead, use a mix of letters and numbers that don't have an obvious meaning.
- Never put personal information (Social Security numbers, bank account or credit card numbers, passwords) in an e-mail unless you're using encryption software.
- If sending personal information over the Internet, make sure that the form is secure. A common symbol for a secure form is a closed padlock in the bottom of your browser window. Also, look for a secure Web address that starts with <https://> instead of <http://>. If you're not sure that the form is secure, don't send your information and look for a telephone number instead.
- Look at a Web site's privacy policy to see how the site uses the information you give them.
- Sites are not supposed to collect more information about you than they need for the activity you want to participate in. You should be able to participate in many activities online without having to give any information about yourself.
- If a site makes you uncomfortable or asks for more information than you want to share, leave the site.
- Use the browser's cookie notification feature and don't accept cookies from places you don't trust.
- Opt out of sharing your information with third parties.
- Don't reply to spam (i.e., unwanted e-mail)—it will just confirm your address for them.
- Create a separate e-mail address to use when filling out forms.
- Don't give out your full name, address, phone number, or location in chat rooms.
- Know that spyware (i.e., hidden programs that track your computer usage) exists and is probably lurking on your computer. Use one of the free utilities like [Ad Aware](http://www.lavasoftusa.com/software/adaware/) (<http://www.lavasoftusa.com/software/adaware/>) or [Spyware Blaster](http://www.javacoolsoftware.com/spywareblaster.html) (<http://www.javacoolsoftware.com/spywareblaster.html>) to periodically check your computer and remove unwanted programs.

For families:

- Parents and children should use the Internet together. If parents are unavailable, they should talk with their children about the sites that were visited.
- The [Children's Online Privacy Protection Act](http://www.ftc.gov/bcp/online/pubs/buspubs/coppa.htm) (<http://www.ftc.gov/bcp/online/pubs/buspubs/coppa.htm> ; COPPA) governs how Web sites and online services may collect and use personal information about children. Under COPPA, Web sites and online services directed to children under age 13 must do the following:
 - Post a privacy policy at all access points to the Web site or service.
 - List the type of information collected from children, and explain how it's collected—through direct questions, through cookies, etc.
 - Explain how the information will be used by the Web site and whether it will be provided to third parties.
 - Provide parents with contact information—address, phone number, and e-mail address—for all sites and services collecting or maintaining children's personal information.
 - Get permission from parents before collecting, using, or disclosing personal information about a child.
 - Allow parents to review, correct, and delete information about their children collected by sites and services.
 - Maintain reasonable procedures "to protect the confidentiality, security, and integrity of personal information collected from children."
- Families should consider having both parents and children sign family "Internet contracts" such as those developed by the [GetNetWise](http://www.getnetwise.org/) (<http://www.getnetwise.org/>) program. See: [Tools for Families: Make an Internet Use Agreement with Your Child](http://kids.getnetwise.org/tools/toolscontracts) (<http://kids.getnetwise.org/tools/toolscontracts>).

If you have a complaint about privacy violations:

- Contact the [Federal Trade Commission](http://www.ftc.gov/) (<http://www.ftc.gov/>) and click on [File a Complaint](https://rn.ftc.gov/pls/dod/wsolcq$.startup?Z_ORG_CODE=PU01) ([https://rn.ftc.gov/pls/dod/wsolcq\\$.startup?Z_ORG_CODE=PU01](https://rn.ftc.gov/pls/dod/wsolcq$.startup?Z_ORG_CODE=PU01)).
- Contact your state attorney general's office for guidance on [privacy laws in your state](http://www.ala.org/oif/stateprivacylaws) (<http://www.ala.org/oif/stateprivacylaws>).

Selected links:

[Privacy Rights Clearinghouse, esp. the "Fact Sheet 18: Online Privacy"](http://www.privacyrights.org/fs/fs18-cyb.htm)
(<http://www.privacyrights.org/fs/fs18-cyb.htm>)

["Fact Sheet 21: Children's Online Privacy"](http://www.privacyrights.org/fs/fs21-children.htm) (<http://www.privacyrights.org/fs/fs21-children.htm>)
"May be copied and distributed for nonprofit, educational purposes only"

[Privacy Tips from the Federal Trade Commission](http://www.ftc.gov/bcp/online/pubs/alerts/privtipsalrt.htm)
(<http://www.ftc.gov/bcp/online/pubs/alerts/privtipsalrt.htm>)

[Top Ten Online Privacy Tips from LearnTheNet.com](http://www.learnthenet.com/english/html/63privtips.htm)
(<http://www.learnthenet.com/english/html/63privtips.htm>)

[Privacy Tips from the Better Business Bureau Online](http://www.bbbonline.org/understandingprivacy/toolbox/tips.asp)
(<http://www.bbbonline.org/understandingprivacy/toolbox/tips.asp>)

[The Electronic Frontier Foundation Top 12 Privacy Tips](http://www.eff.org/Privacy/eff_privacy_top_12.html)

(http://www.eff.org/Privacy/eff_privacy_top_12.html)

[The Center for Democracy & Technology Top 10 Ways to Protect Privacy](http://www.cdt.org/privacy/guide/basic/topten.html)

(<http://www.cdt.org/privacy/guide/basic/topten.html>)

[12 Principles for Fair Commerce in Software and Other Digital Products](http://www.fairterms.org/12PrincGeneral.htm)

(<http://www.fairterms.org/12PrincGeneral.htm>)

Privacy Tool Kit

<http://www.ala.org/ala/oif/iftoolkits/toolkitsprivacy/privacy.htm>

Legislative Advocacy for Privacy and Civil Liberties

Make Yourself Heard

Today, many legislative actions and court decisions undermine patron privacy and chill the use of libraries and information resources. Such measures have profound implications for libraries, user policies, and privacy:

Learn More about the Issues

Link to ALA's Washington Office Web pages for

- Information about [pending legislation and its impact on libraries](http://www.ala.org/template.cfm?Section=washoff) (<http://www.ala.org/template.cfm?Section=washoff>)
- ALA resolutions that support or oppose legislative actions
- Bill status

Link to Office for Intellectual Freedom pages for

- Information about [privacy](http://www.ala.org/ala/oif/statementspols/statementspolicies.htm#privacy) (<http://www.ala.org/ala/oif/statementspols/statementspolicies.htm#privacy>) and the impact of various legislative and judicial actions on free expression
- ALA resolutions reaffirming the principles of intellectual freedom and confidentiality of library records
- [Privacy: An Interpretation of the Library Bill of Rights](http://www.ala.org/oif/policies/interpretations/privacy) (<http://www.ala.org/oif/policies/interpretations/privacy>)
- [Privacy Tool Kit](http://www.ala.org/oif/iftoolkits/privacy) (<http://www.ala.org/oif/iftoolkits/privacy>)
- [State Privacy Laws Regarding Library Records](http://www.ala.org/oif/stateprivacylaws) (<http://www.ala.org/oif/stateprivacylaws>)
- [Confidentiality and Coping with Law Enforcement Inquiries: Guidelines for the Library and its Staff](http://www.ala.org/oif/ifissues/lawenforcementinquiries) (<http://www.ala.org/oif/ifissues/lawenforcementinquiries>)

Link to Freedom to Read Foundation pages for

- Information from the [Freedom to Read Foundation](http://www.ftrf.org) (<http://www.ftrf.org>), which is particularly interested in protecting patron privacy and curtailing expanded government surveillance powers in libraries and bookstores

Do More

1. Keep informed and up to date.
2. Educate library boards and staff, communities, the media and local governments.
 - Write newspaper articles, guest editorials and letters to the editor
 - Make presentations to local and civic organizations

- Keep government officials up to date
- 3. Gather information about impact on local communities by compiling binders or Web site links concerning effects of laws and governmental actions that infringe on civil liberties and privacy.
- 4. Organize a publicity campaign.
 - Prepare brochures and handouts to explain local and national impacts
 - Take out ads in your association's newsletters and journals and the local newspapers
- 5. Organize town meetings and public forums.
- 6. Cooperate with other interested organizations like the ACLU, AAUW, League of Women Voters, Common Cause, religious and civic groups, and local bar associations in discussions about how to counter the sections of the laws that infringe on civil liberties
- 7. Make information available to those, such as library boards and organizations, local governmental bodies and others, who want to pass resolutions opposing these laws (or parts of them) and related matters
- 8. [Form or join coalitions](http://www.ala.org/Template.cfm?Section=basicrelatedlinks&Template=/ContentManagement/ContentDisplay.cfm&ContentID=11699)
- 9. [Contact legislators at the federal, state and local levels](http://www.ala.org/ala/oif/basics/basicrelatedlinks/contactingelected.htm) (<http://www.ala.org/ala/oif/basics/basicrelatedlinks/contactingelected.htm>) to persuade lawmakers to amend and change laws that infringe on civil liberties.
 - Attend National Library Legislative Day sponsored by ALA and DCLA
 - Attend your state legislative day
 - Establish a personal relationship with your federal, state and local legislators and staff.
 - Write letters and include resolutions passed by your professional organization
- 10. Require accountability from law enforcement agencies
 - Ask local law enforcement officials to speak to local organizations, town meetings and participate in programs at your library
 - Keep abreast of local law enforcement activities concerning civil liberties and privacy.
- 11. Encourage libraries to join court challenges.
 - Investigate appropriateness of joining other groups' initiated court challenges
 - Keep informed about court cases such as the denial of Freedom of Information Act requests for information about surveillance of library users
- 12. Make your community a Civil Liberties Safe Zone. For guidance, see the [Bill of Rights Defense Committee](http://www.bordc.org/) (<http://www.bordc.org/>).

See also:

American Library Association, Washington Office. ["What to Do About Laws and Government Actions That Infringe on Civil Liberties and Privacy."](http://www.ala.org/ala/washoff/WOissues/civilliberties/theusapatriotact/patriottips.pdf) (<http://www.ala.org/ala/washoff/WOissues/civilliberties/theusapatriotact/patriottips.pdf>) (Washington, DC: ALA Washington Office, January 2003).

Privacy Tool Kit

<http://www.ala.org/ala/oif/iftoolkits/toolkitsprivacy/privacy.htm>

SELECTED PROFESSIONAL BIBLIOGRAPHY*

Selected Background Readings & Reference Works

Computer Professionals for Social Responsibility, Cyber-Rights Working Group. "Electronic Privacy Principles (<http://www.cpsr.org/issues/privacy/epp>)." **Approved by the CPSR Board Sept. 3, 1996.**

This site provides a general overview of online privacy concerns, then lists the privacy protection responsibilities of various groups, including employers, service and information providers, software developers, governments, individuals, and others. Includes links to other sources, but most are broken. Useful as an example of earlier online privacy statements.

Garfinkel, Simson. Database Nation. O'Reilly & Associates, 2000.

This book is intended as a call to action. Looking at (among other things) satellites, supermarket club cards, and Social Security numbers, Garfinkel outlines the varied threats to privacy that are embedded in daily life. Suggests how current laws (pre-USA PATRIOT Act) may be modified to preserve privacy rights.

Miller, Seumas. "Privacy, Data Bases, and Computers." Journal of Information Ethics. 7 (1), Spring 1998: 42-48.

A concise overview of the philosophical aspects of privacy is followed by a prescient concern about the potential and real abuses of the increasing amount of personal information collected and aggregated by computer databases.

Mintz, Anne, ed. Web of Deception. CyberAge Books, 2002.

Various experts describe the critical thinking skills needed to evaluate Internet and emailed charity solicitations, legal advice, medical advice, fraud, misinformation, identity theft and other threats to privacy or accuracy in Web-searching and information-gathering.

Privacy and Human Rights: An International Survey of Privacy Laws and Developments. Electronic Privacy Information Center & Privacy International. Published annually since 1999.

Issued jointly by two important privacy advocacy groups, PHR reviews the state of privacy in over fifty countries, outlining the conditions under which privacy is protected and summarizing recent events. Some of the topics covered include data protection, wiretapping and surveillance, genetic databases, ID systems, freedom of information laws, and workplace privacy rights. Full Web accessibility (at <http://www.privacyinternational.org/survey/>) helps make this an important resource for tracking legal and international developments.

Rosen, Jeffrey. *The Unwanted Gaze: The Destruction of Privacy in America*. Random House, 2000.

In this book, Rosen examines the erosion of privacy in different arenas: home, work, law, the courts, and cyberspace. In all of these areas, technology plays a central role in the loss of privacy. The author demonstrates that the failure of privacy protections to keep pace with technological advances in communication is the primary culprit behind the loss of privacy.

Raul, Alan Charles. *Privacy and the Digital State: Balancing Public Information and Personal Privacy*. Kluwer, 2002.

This book explores the issues of privacy and government services. Acknowledging the benefits of digital government services at the outset, Raul then outlines the flaws in current privacy law, examines constitutional foundations for existing legislation, and suggests best practices for governments. Examples of state policies are also included.

Rotenberg, Marc, editor. *Privacy Law Sourcebook: United States Law, International Law, and Recent Developments*. Electronic Privacy Information Center. Published annually since 1999.

This work intends to provide a "basic set of privacy materials for the US and the international sphere." Reprints privacy law and treaties from around the world, and includes sections covering recent developments and threats to privacy. Some items not reprinted from year to year; access to old volumes can be useful.

Warren, Samuel & Brandeis, Louis. "The Right to Privacy." *Harvard Law Review*. 4 (5), Dec. 1890: 193-220.

Source of "the right to be let alone," this foundational document has been called one of the most influential essays in the history of American law. Reflecting the upper class concerns of its day, it addresses commercial exploitation of gossip and technological aids to an invasive press, rather than Big Brother government surveillance.

Selected Readings on Privacy & Confidentiality in Librarianship

Adams, Helen R. "Privacy & Confidentiality: Now More Than Ever Youngsters Need to Keep Their Library Use Under Wraps." *American Libraries*. Nov. 2002: 44-48.

In this article, youth services librarians and school media specialists give examples of the privacy concerns faced by today's children and youth. A review of state and federal legislation that impacts privacy is also included, along with suggestions for training both students and staff about privacy.

Angel, Colleen. "The Right to Privacy." *Journal of Information Ethics*. 9 (2), Fall 2000: 11-25.

Tracing the right to privacy back to the Magna Carta, this article outlines the historical development of privacy rights, lists current threats and violations to established privacy rights, and identifies areas of action for maintaining our historic rights.

Bielefield, Arlene. *Maintaining the Privacy of Library Records: A Handbook and Guide*. Neal-Schuman, 1994.

This book provides an excellent overview of the relationship between libraries and the First Amendment, the constitutional right to privacy, and major federal laws that protect privacy. This book also includes a state-by-state comparison of library privacy protections, along with the actual legislation. However, any changes in the last ten years are absent, so this section of the book is not reliable.

Coyle, Karen. "[Privacy and Library Systems Before & After 9/11](http://www.kcoyle.net/stbarb.html) (<http://www.kcoyle.net/stbarb.html>): Outline of talk given March 27, 2002 at the Public Library Directors' Forum."

These notes provide some guidance for reviewing policies and procedures regarding information collected and stored by library information systems. Suggestions for proactively addressing privacy issues both within and beyond the library are also discussed. More recent papers are available from: <http://www.kcoyle.net/>.

Estabrook, Leigh S. "[Public Libraries' Response to the Events of September 11th](http://www.lis.uiuc.edu/gslis/research/national.pdf) (<http://www.lis.uiuc.edu/gslis/research/national.pdf>), A National Survey Conducted by the Library Research Center at the University of Illinois Graduate School of Library and Information Science." Library Research Center, Graduate School of Library and Information Science, University of Illinois at Urbana Champaign. January 22, 2003.

This survey of Illinois public libraries examined changes in security policies, collection development, and staff behavior regarding patron Internet usage and privacy issues. Awareness of the USA PATRIOT Act was also measured. This and additional studies can be found at: <http://alexia.lis.uiuc.edu/~leighe/>.

Fifarek, Aimee. "Technology and Privacy in the Academic Library." *Online Information Review*. 26 (6), 2002: 366-374.

This essay addresses privacy threats arising from the ever-increasing adoption of new information technologies in academic libraries. The author provides a systems librarian's perspective on the interaction between librarians on the one hand and campus computing and campus police on the other. Fifarek provides a case study in "privacy failure," discusses both clear and unclear aspects of privacy-related legislation (including the USA PATRIOT Act), provides a list of measures that librarians can take to protect their patrons, and concludes with suggestions on creating acceptable use policies.

Gardner, Carrie. "[Fact or Fiction: Privacy in American Libraries](http://www.cfp2002.org/proceedings/proceedings/gardner.pdf) (<http://www.cfp2002.org/proceedings/proceedings/gardner.pdf>)." Presented at **Computers, Freedom and Privacy 2002**.

This paper provides examples of how libraries and ALA have historically protected patrons' privacy, then outlines some concerns about privacy and the Internet. It also includes a draft of "[Privacy: An Interpretation of the Library Bill of Rights](http://www.ala.org/oif/policies/interpretations/privacy) (<http://www.ala.org/oif/policies/interpretations/privacy>)."

Gorman, Michael. "[Privacy in the Digital Environment: Issues for Libraries \(PDF\)](#)." Presented at IFLA Council and General Conference 2001.

The ever-growing impact of technology on privacy, especially in libraries, is examined in this paper. Gorman outlines the historical development of the concept of privacy, examines issues raised by technological advances, and challenges some common library practices that don't follow the profession's historical standards.

Guenther, Kim. "Pass the Cookies and Uphold the Privacy." *Computers in Libraries*. 21 (6), June 2001: 56-58.

This article identifies personal profiling trends within libraries and suggests policies for protecting patron privacy. Guidelines from TRUSTe and the Organisation for Economic Cooperation and Development are discussed.

Hildebrand, Janet. "Is Privacy Reserved for Adults? Children's Rights at the Public Library." *School Library Journal* (37), Jan. 1991: 21-5.

This article addresses some of the common concerns related to children's privacy at the library, such as financial responsibility, parental rights, and age of consent. Examples of how two public libraries have approached these issues are provided, along with clear explanations of the ethical issues involved.

International Coalition of Library Consortia. "[Privacy Guidelines for Electronic Resources Vendors](http://www.library.yale.edu/consortia/2002privacyguidelines.html) (<http://www.library.yale.edu/consortia/2002privacyguidelines.html>)," July 2002.

These guidelines are a template for helping database publishers and vendors develop appropriate policies for safeguarding patron privacy. Included is a sample privacy policy statement to be used by publishers and vendors.

McFall, Mairi & Karen Schneider. "[The USA Patriot Act And What You Can Do](http://www.cla-net.org/resources/articles/us_patriot_act.php) (http://www.cla-net.org/resources/articles/us_patriot_act.php)." **California Library Association, 2003.**

From the CLA Intellectual Freedom Committee, this concise document provides an overview of the Act, gives suggestions for responding to law enforcement requests, and has a great twelve point checklist for identifying potential stores of information in common library technology. Suggested resources for further research are provided.

Minow, Mary. "[The USA PATRIOT Act and Patron Privacy on Library Internet Terminals](http://www.llrx.com/features/usapatriotact.htm) (<http://www.llrx.com/features/usapatriotact.htm>)." **Published Feb. 15, 2002.**

Minow, a library law consultant, answers frequently asked questions about librarians' professional and ethical responsibilities under the USA PATRIOT Act. Legal obligations under provisions of the Act are reviewed and recommendations are included.

Murray, Peter E. *Library Patron Privacy. SPEC Kit, 278. Association of Research Libraries, 2003.*

Fifty-eight ARL member libraries (47% of ARL) responded to a 2003 survey on Library Patron Privacy. Survey results are presented with sample privacy policies for general library policies,

circulation record, Web site, interlibrary loan, electronic reference, public access computers, hardware repair and disposal, and patron record requests.

Neuhaus, Paul. "Privacy and Confidentiality in Digital Reference." *Reference & User Services Quarterly*. 43 (1), Fall 2003: 26-36.

Digital reference includes chat reference, e-mail reference, Web forms, automated reference agents, knowledge bases and FAQ's, and transaction logs. The privacy issues for each type are discussed, and legal and ethical underpinnings of privacy policies are reviewed.

Peace, A. Graham & Kathleen S. Hartzel. "Ethical Concerns Raised by the Use of the Internet in Academia." *Journal of Information Ethics*. 11 (2), Fall 2002: 17-32.

In a broad look at the Internet's impact on a range of issues, including intellectual property, freedom of speech, and accessibility, this article also examines the interaction between privacy and technology as currently employed in higher education.

"Should Libraries Play Tag with RFIDs?" *American Libraries*. 34 (11), Dec. 2003: 69-71.

This interview with librarians Jackie Griffin and Karen Schneider outlines both advantages and concerns of using radio frequency identification (RFID) technology in library applications.

Sturges, Paul Vincent Teng, Ursula Iliffe et al. "User Privacy in the Digital Library Environment: An Investigation of Policies and Preparedness." *Library Management*. 24 (1/2), 2003: 44-50.

Surveys were conducted in the United Kingdom of library users, libraries, and vendors of library management software on the privacy of digital library records. A significant disparity was found between users' expectations of the privacy of library records and libraries' preparedness to protect privacy. This study is useful for examining how another society views privacy.

Tavani, Herman. "Privacy-Enhancing Technologies as a Panacea for Online Privacy Concerns: Some Ethical Considerations." *Journal of Information Ethics*. 9 (2), Fall 2000: 26-36.

The development of Privacy-Enhancing Technologies (PET's), or technical and organizational concepts aimed at protecting personal identity, raises several ethical questions rather than solving privacy concerns. Viewing privacy as a commodity or a basic human right may give quite different perspectives on the need for education, informed consent, and social equity in the collection and use of personal information.

Vandergrift, Kay E. "Privacy, Schooling and Minors." *School Library Journal* (37), Jan. 1991: 26-30.

The author addresses a number of ways in which student privacy rights are routinely violated in the school setting, ending by addressing the role of the school library media specialist in protecting these rights.

Weiner, Robert G. "[Privacy and Librarians: An Overview](http://www.txla.org/pubs/tlj-1q97/privacy.html) (http://www.txla.org/pubs/tlj-1q97/privacy.html)." *Texas Library Journal*. 73 (1), Spring 1997.

An overview of various privacy concerns in libraries is provided, with reference to legal cases and their significance.

Wiegand, Shirley A. *Library Records: A Retention and Confidentiality Guide*. Greenwood Press, 1994.

State-by-state reviews of public record retention laws as they apply to library records are provided, with recommendations to enact strong confidentiality policies and laws.

Winter, Kenneth A. "[Privacy and the Rights and Responsibilities of Librarians](http://alexia.lis.uiuc.edu/review/winter1997/winter.html) (http://alexia.lis.uiuc.edu/review/winter1997/winter.html)." *The Katharine Sharp Review* (No. 4), Winter 1997.

Winter gives an overview of the court decisions from which privacy has been interpreted as a Constitutional right, and discusses privacy issues in various types of libraries by reviewing specific cases.

*Note that items previously cited in the Privacy Tool Kit are not listed here.