## **DRAFT: Privacy: An Interpretation of the *Library Bill of Rights***

Privacy is essential to the exercise of free speech, free thought, and free association. The courts have established a First Amendment right to receive information in a publicly funded library.[[1]](#footnote-0) Further, 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.[[2]](#footnote-1) Numerous decisions in U.S. case law have defined and extended rights to privacy.[[3]](#footnote-2)

The right to privacy is the right to open inquiry without having the subject of one’s interest examined or scrutinized by others, in person or online. Confidentiality exists when a library is in possession of personally identifiable information about users and keeps that information private on their behalf.[[4]](#footnote-3) Article III of the ALA *Code of Ethics* states that confidentiality extends to “information sought or received and resources consulted, borrowed, acquired or transmitted,” including, but not limited to reference questions and interviews, circulation records, digital transactions and queries, as well as records regarding the use of library materials, services, programs, or facilities.

Protecting user privacy and confidentiality has long been an integral part of the mission of libraries. The ALA has affirmed a right to privacy since 1939.[[5]](#footnote-4) Existing ALA policies affirm that confidentiality is crucial to freedom of inquiry. Rights to privacy and confidentiality are explicit in Article VII of the [*Library Bill of Rights*](http://www.ala.org/advocacy/sites/ala.org.advocacy/files/content/intfreedom/librarybill/lbor.pdf) and implicit in its guarantee of free access to library resources for all users.

### **Rights of Library Users**

Article VII of the *Library Bill of Rights* states, “All people, regardless of origin, age, background, or views, possess a right to privacy and confidentiality in their library use.” When users recognize or fear that their privacy or confidentiality is compromised, true freedom of inquiry no longer exists. Lack of privacy and confidentiality has a chilling effect on users’ selection, utilization, and access to library resources.

All users, including students and minors, have a right to be free from any unreasonable intrusion into or surveillance of their lawful library use. ALA and its members recognize that children and youth have the same rights to privacy as adults. Library users expect, and in many places have, a legal right to have their personally identifiable information and library use data protected and kept private and confidential by anyone with direct or indirect access to that information.

### Libraries have a responsibility to inform users about policies and practices governing the collection, security, and retention of personally identifiable information and library use data. Additionally, users should have the choice to opt-in to any data collection that is not essential to library operations, and the opportunity to opt-out again at any future time. In all areas of librarianship, best practice leaves users in control of as many choices as possible regarding their privacy. This includes decisions about the selection of, access to, and use of information.

### **Responsibilities in Libraries**

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

Libraries should not monitor, track, or profile an individual’s library use. Data collected for analytics use should be limited to anonymous or aggregate data and not tied to an individual’s library use. Emerging biometric technologies, such as facial recognition, are inconsistent with the mission of facilitating access to library resources, free from any unreasonable intrusion into or surveillance of an individual’s library use.

Personally identifiable information and library use data should only be collected and maintained when necessary for the provision of library services. Regardless of the technology used, everyone who collects or accesses personally identifiable information in any format has a legal and ethical obligation to protect confidentiality. Library security practices to safeguard personal information should be up to date and in compliance with state and national standards. Adherence to *NISO Consensus Principles on Users’ Digital Privacy in Library, Publisher, and Software-Provider Systems* requires that these practices include:

encryption of personal data while they are at-rest and in-motion; prompt updates of systems and software to address vulnerabilities; systems, procedures, and policies for access control of sensitive data; a procedure for security training for those with access to data; and documented procedures for breach reporting, incident response, and system, software, and network security configuration and auditing.[[6]](#footnote-5)

Libraries should follow purpose limitation, storage limitation, and data minimization principles[[7]](#footnote-6) when making decisions about collecting and retaining library use data. In particular, libraries should collect and store only personally identifiable data that are required for specific purposes that are disclosed to the users.

Libraries should periodically review their data collection and retention policies to identify situations in which the reason for collecting user data may no longer apply. In addition, libraries should regularly review and update procedures for collecting and maintaining user data to ensure compliance with current industry privacy and security standards.

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

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

The American Library Association affirms that rights of privacy are necessary for intellectual freedom and are fundamental to the ethical practice of librarianship. The rapid pace of information collection and changes in technology means that users’ personally identifiable information and library use data are often at increased risk of exposure. The use of new technologies in libraries that rely on the collection, use, and sharing of user data may come into direct conflict with the Library Bill of Rights and librarians’ ethical responsibilities. Similarly, new technologies that monitor or track users’ activities may directly conflict with the Library Bill of Rights and librarians’ ethical responsibilities. Libraries should consider privacy in the design and delivery of all programs and services, paying careful attention to their own policies and procedures and that of any vendors with which they work. Privacy is the foundation upon which our libraries were built and the reason that libraries are such a trusted part of every community.

Adopted June 19, 2002, by the ALA Council; amended on July 1, 2014.

1. Court opinions establishing a right to receive information in a public library include *Board of Education v. Pico*, 457 U.S. 853 (1982); *Kreimer v. Bureau of Police for the Town of Morristown*, 958 F.2d 1242 (3d Cir. 1992); and *Reno v. American Civil Liberties Union*, 117 S.Ct. 2329, 138 L.Ed.2d 874 (1997). [↑](#footnote-ref-0)
2. Ten state constitutions guarantee a right of privacy or bar unreasonable intrusions into citizens’ privacy. Forty-eight states protect the confidentiality of library users’ records by law, and the attorneys general in the remaining two states have issued opinions recognizing the privacy of users’ library records. See: [State Privacy Laws Regarding Library Records](http://www.ala.org/advocacy/privacy/statelaws). [↑](#footnote-ref-1)
3. Cases recognizing a right to privacy include: *NAACP v. Alabama*, 357 U.S. 449 (1958); *Griswold v. Connecticut*,381 U.S. 479 (1965); *Lamont v. Postmaster General*, 381 U.S. 301 (1965); *Katz v. United States*, 389 U.S. 347 (1967); and *Stanley v. Georgia*, 394 U.S. 557 (1969). [↑](#footnote-ref-2)
4. The phrase “personally identifiable information” was adopted by the ALA in 1991. See: “[ALA Policy Concerning Confidentiality of Personally Identifiable Information about Library Users](http://www.ala.org/advocacy/intfreedom/statementspols/otherpolicies/policyconcerning).”  [↑](#footnote-ref-3)
5. Article Eleven of the Code of Ethics for Librarians (1939) asserted that “It is the librarian’s obligation to treat as confidential any private information obtained through contact with library patrons.” See: Code of Ethics for Librarians (1939). Article Three of the 1995 ALA Code of Ethics states: “We protect each library user’s right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired, or transmitted.” [↑](#footnote-ref-4)
6. [NISO Consensus Principles on Users’ Digital Privacy in Library, Publisher, and Software-Provider Systems (NISO Privacy Principles) (2015)](https://groups.niso.org/apps/group_public/download.php/16064/NISO%20Privacy%20Principles.pdf) [↑](#footnote-ref-5)
7. [European Union General Data Protection Regulation (2018)](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN) [↑](#footnote-ref-6)