

Library Privacy Policy Statement (Final Policy Recommendation Approved by MnSCU)

It is the policy of the Livingston Lord Library of Minnesota State University Moorhead to respect the privacy of its patrons to the extent permitted by law. The Library's privacy practices are consistent with applicable state and federal privacy laws including, but not limited to, the Minnesota Government Data Practices Act ([MGDPA](#), Minnesota Statutes Chapter 13) and the Family Educational Rights and Privacy Act ([FERPA](#), 20 U.S.C. 1232g), as well as professional standards of the [American Library Association](#). Minnesota State University Moorhead is part of the Minnesota State College and University System and is subject to its Board Policies and Procedures, which may be found at: <http://www.mnscu.edu/board/policy/index.html>

The following information maintained by the Library are private data on individuals and may not be disclosed for other than library purposes except pursuant to a court order, or as otherwise required or permitted by law:

1. Data that link a Library patron's name with materials requested or borrowed by the patron or that link a patron's name with a specific subject about which the patron has requested information or materials; or
2. Data in applications for borrower cards, other than the name of the borrower.

Additional information about your data rights as an individual and the university's responsibilities concerning the handling of private data may be found as the following website: [MSU Moorhead Campus-Wide Guidelines For Computer And System Use: Responsible Behavior And The Electronic Media Data Privacy And Security](#)

Retention Policies

Information we may gather and retain about current and valid library users include the following:

User Registration Information is maintained indefinitely in the current Library catalog software. In the future, some User Information may automatically delete when the system is upgraded to newer software versions.

Circulation Information is not kept in the form of a permanent ongoing record of borrowing for any individual. Once materials are returned, that record is deleted. However, the Library system's back-up files may retain borrowing information for up to 60 days after an item is returned. Records where fines have been incurred are maintained indefinitely.

Electronic Access Information is not made available to any other entity outside the Library except as required by law. The Library maintains statistics only of database usage statistics.

Information Required to Provide Library Services such as consultation services in the form of reference or research consultation will only be shared outside the Library with third parties under certain circumstances as required or permitted by law. InterLibrary Loan service necessitates the sharing of patron information

between libraries, but will only be disclosed during these transactions if necessary to conduct Library business.

Online Privacy Practices

The policy of the Livingston Lord Library at Minnesota State University Moorhead is to respect the privacy of all web site visitors to the extent permitted by law. This online privacy statement is intended to inform you of the ways in which this web site collects information, the uses to which that information will be put, and the ways in which we will protect any information you choose to provide us.

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; destroying untimely data.

Data Retention: We protect personally identifiable information from unauthorized disclosure once it is no longer needed to manage library services.

Tracking Users: The system removes links between patron records and materials borrowed when items are returned and records are deleted as soon as the original purpose for data collection has been satisfied, with the exception of fines. Currently, the system default for all MnPALS Libraries is 60 days. We permit in-house access to information in all formats without creating a data trail. 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. The computers in the Library currently operate under a software program which reverts the hard drive back to its original state after two hours of inactivity. At a minimum, this process is done daily.

Third Party Security: We strive to ensure that our Library's contracts, licenses, and offsite computer service arrangements reflect our policies and legal obligations concerning user privacy and confidentiality. When connecting to licensed databases outside the Library, we release only information authenticating users as "members of our community."

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.

MSUM web sites provide links to other World Wide Web sites or resources. We do not control these sites and resources, do not endorse them, and are not responsible for their availability, content, or delivery of services. In particular, external sites are not bound by the University's online privacy policy; they may have their own policies or none at all. Often you can tell you are leaving a University web site by noting the URL of the destination site.

[Minn. Stat. 13.15](#) provides that electronic access data may be disseminated: (1) to the commissioner for the purpose of evaluating electronic government services; (2) to another government entity to prevent unlawful intrusions into government electronic systems; or (3) as otherwise provided by law.

Enforcement & Redress

Our Library will not share data on individuals with third parties, including law enforcement, unless required or permitted by law. There are certain provisions of the [USA PATRIOT Act](#) which can allow law enforcement officials to request information without your knowledge. Library users who have questions, concerns, or complaints about the Library's handling of their privacy and confidentiality rights should file written comments with the Director of the Instructional Resources. We will respond in a timely manner and may conduct a privacy investigation or review of policy and procedures.

We authorize only the Associate Vice President of Instructional Resources, our Vice President of Academic Affairs, and our Director of Campus Security to receive or comply

with requests from law enforcement officers; we confer with our legal counsel before determining the proper response. In most cases, 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.

This policy is closely adapted from ALA's Model Privacy Policy at <http://www.ala.org/ala/aboutala/offices/oif/iftoolkits/toolkitsprivacy/guidelinesfordevelopinglibraryprivacypolicy/guidelinesprivacypolicy.cfm>

Adopted 9/15/2006