

Library Privacy Statements and Policies

UC Irvine Libraries Privacy Statement

Last updated: August 17, 2004

The UC Irvine Libraries provide the Libraries Web site and services to facilitate the pursuit and production of knowledge in support of learning and scholarship at the University of California, Irvine. Your privacy while using the UC Irvine Libraries Web site and services is an important element of intellectual and academic freedom. UC Irvine Libraries are committed to protecting the privacy of our library users. Our policies also support the [California Digital Libraries commitment to user privacy](#) and the precepts of confidentiality described in the [Code of Ethics of the American Library Association](#), which 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."

Confidentiality of Library Records

In the course of providing services, such as Library Search, Interlibrary Loan, and reference services, the Libraries acquire personally identifiable information about you, including your name, university ID, and items borrowed. When it is necessary for the Libraries to identify users in the course of normal library business, it is our goal to keep personal information for the shortest amount of time necessary to complete transactions or provide service. Access to personal information is restricted to authorized library staff who need it to conduct library business. Personal information is never revealed to external parties unless required by law and never used for commercial purposes. The Libraries adhere to the [UCI Guidelines for the UC Electronic Communications Policy](#), [campus and UC policies](#), and [state and national laws](#).

Library Search

In order for the UCI community to conduct business with the Libraries (e.g., library circulation records, "My Library Account" portal service, interlibrary loan requests), the Libraries maintain a patron database in the Library Search that stores personal information. Transaction records are deleted from the Library Search system after each transaction is completed. Inactive patron records are periodically removed from the patron database. The Libraries use the information in your patron records only to interact with and provide service to you (e.g., fulfilling interlibrary borrowing requests, placing holds, and collecting overdue fines). Browsing Library Search to look up titles and check book and journal locations does not require any personal information from you.

UC Irvine Libraries Web Site


The UC Irvine Libraries routinely collect information to help us manage the site and improve service. Examples of such information collected and stored by the UC Irvine Libraries Web site include:

- your Internet location (Internet domain and IP address)
- type of browser and operating system used to access our site
- date and time our site was visited
- pages visited on our site
- search terms used on our search engines

The UC Irvine Libraries Web site links to other sites and resources that are not under the administrative control of UC Irvine Libraries. These external sites may have privacy policies that are different from UC Irvine Libraries or none at all. UC Irvine Libraries cannot guarantee the privacy policies of these sites. Where the Libraries contract with vendors for digital information products and resources, every attempt is made to include user privacy protections in the license agreements. Often you can tell you are leaving a UC Libraries Web site by noting the URL of the destination site. We encourage you to read the privacy statements at these sites to determine their privacy practices.

Related Policies

- [User Rights and Responsibilities](#)
- [Ask a Librarian Privacy Statement](#)



[My Accounts](#)[Ask a Librarian](#)

[Search & Find](#)[Using the Library](#)[Research Support](#)[Course Support](#)[Libraries](#)[About](#)

[Home](#) > [About](#) > [Privacy](#)

Privacy

What kinds of information do the Libraries collect?

When you use this website, the Libraries' web server collects technical information from your web browser, including:

- browser type
- internet address
- operating system type
- web address of the page from which you linked to our site

We also use [Google Analytics](#), which uses cookies, for statistical analysis related to your browsing behavior on the Libraries' websites. In some cases our web server may use browser cookies or other technologies to maintain session and preference information.

How do the Libraries use this information?

Information that we automatically collect via this website is used internally for the following:

- improving the usability of our website
- technical troubleshooting
- tracking aggregate statistical trends

Do the Libraries collect my personal information?

We do not collect any personally identifiable information, such as your:

- age
- address
- gender
- ID numbers
- name
- phone number

OUR COMMITMENT TO YOU

One of the cornerstones of librarianship is respect for the privacy of library users. Duke University Libraries recognize the importance of protecting your privacy and the confidentiality of the information you share with us when you use our websites or other library services. On this page you will find our policy on collecting, disclosing, maintaining, protecting and using your personal information.

But what about personal information I submit via a web form or an e-mail message?

We interact with our library users regularly and receive personal information via email messages, chat sessions, web forms and other communications. If you submit personal information via one of these platforms, we:

- use your information for the purpose for which you submitted it only
- will not use your personal information for any other purpose
- will not combine your personal information with [the other types of information we collect](#)
- do not disclose to third parties any information that could be used to identify you or your use of Duke University Libraries resources, except as required by law or appropriate law enforcement procedures

What about the personal information in my online library account?

The Duke University Libraries maintain personally identifiable information in the online accounts of valid library users. For example:

- We receive personal information from the Registrar's Office (for students) and from Human Resources (for employees) in order to create and update the library accounts of users affiliated with Duke University.
- We obtain personal information about you in order to create your library account. We will maintain the confidentiality of all information we seek or receive and of the materials you consult, borrow or acquire — such as information related to circulation records; database search records; Interlibrary Request records; Duke University Libraries facilities, materials or services and reference interviews.
- We collect and store personal information you submit via the Libraries' web-based management tools — such as forms related to asking reference questions, requesting and renewing books and saving search histories or resource preferences. We use this information to maintain your library account and to provide services to you. We do not make this information available to any other entity outside the Libraries, except as required by law or appropriate law enforcement procedures.

Can I disable cookies and other tracking technologies?

Yes. You can disable cookies and other web technologies in your browser preference settings. However, please keep in mind that doing so may mean some features of this website will not function properly.

What are the privacy practices of the third-party tools the Libraries use?

Our website contains links to websites and licensed databases that Duke University Libraries does not maintain or support. We use third-party tools for some of our library services (such as online chatting with a librarian and searching for materials via specialized widgets). Please note that Duke University Libraries is not responsible for the privacy practices or the content of these third parties. We encourage you to read the policies associated with these third-party tools before using the tools.

Can I see the information maintained in my library account?

You are entitled to view your library account information and to amend information that is incorrect.

- If you are a student, you can correct your library account information via the Registrar's Office.
- If you are a Duke University employee, you can correct your library account information via Human Resources.
- If you are a patron who has purchased borrowing privileges and who shows proper identification, you can correct your library account information at the library that issued your library card.

Is my information secure?

In general, Internet transactions are not secure because they often are not encrypted. In some cases, however, transactions on our website occur using a SSL (Secure Socket Layer protocol) connection. This provides increased security to the information as it is transmitted. Only authorized library staff with assigned passwords may access personally identifiable information stored in Duke University Libraries' computer systems, and they may do this for the purpose of performing library work only. We use industry-standard security measures to protect any personal information that you may provide to us. However, we cannot guarantee that your submissions to our website, any content residing on our servers or any transmissions from our server will be completely secure.

How will I know if this privacy policy changes?


We will post any substantial changes in this privacy policy at least 30 days prior to the change taking effect. Any information collected under this current policy will remain bound by the terms of this privacy policy. After the changes take effect, all new information we collect, if any, will be subject to the revised privacy policy.

How can I get more information about this policy?

If you have questions about this policy or feel that we have acted in violation of this policy, please contact the [webmaster](#).

Any other information I need to know?

- Duke University Libraries also adheres to Duke University [privacy and computer policies](#) published by the IT Security Office and the Office of Information Technology.
- The [American Library Association](#) provides information about the privacy and confidentiality principles supported by the library profession.









Contact Us

411 Chapel Drive
Durham, NC 27708
(919) 660-5870
Perkins Library
Service Desk


Services for...


Faculty & Instructors	Alumni
Graduate Students	Donors
Undergraduate Students	Visitors
International Students	Patrons with Disabilities



Sign Up for Our Newsletter

Re-use & Attribution / Privacy
Support the Libraries





Library Staff Sign In

Robert W. Woodruff Library

[Home](#) / [Privacy and Related Policies](#) / [Policy on the Collection, Use, and Disclosure of Personal Information](#)

Policy on the Collection, Use, and Disclosure of Personal Information

(Rev. 23 August 2013)

Introduction

Emory University Libraries recognize the importance of freedom of speech and of personal privacy of students, faculty, and other users of the libraries' materials. We endeavor to ensure the privacy of our users' communications, whether by face-to-face, telephone, email or other electronic means.

Use of library facilities whether in person or via computer may produce personally identifiable information (information which can be directly or indirectly tied to a specific person).

Access to personally identifiable information¹ is restricted to Library staff who need it to conduct Library business². Personally identifiable information is never used for commercial purposes and is never revealed to a third party except as required and authorized by policy, law or to comply with a subpoena or court order only with the consent and advice of the University's Legal Counsel. The Library is supported in these practices by national, state and local laws, as well as by University policies.

Except as required by law, users of Library systems and services are informed whenever personally identifiable information other than transactional information will be collected and stored automatically by the system or service. The Libraries retains personally identifiable information only so long as it is required for operational purposes.

The Library does not routinely inspect, monitor, or disclose records of electronic transactions for other than Library business purposes. The Libraries and University Policies prohibit employees and others from seeking out, using or disclosing such information without authorization, and requires employees to take necessary precautions to protect the confidentiality of personally identifiable information encountered in the performance of their duties or otherwise.

Library Web Sites

In the course of providing you with Web-based services, The Library collects and stores certain information automatically through our Web sites. We use this information on an aggregate basis to maintain, enhance or add functionality to our Web-based services. It includes:

EMORY UNIVERSITY LIBRARIES

Policy on the Collection, Use, and Disclosure of Personal Information

<http://web.library.emory.edu/privacy-policy/personal-information.html>

- your Internet location (IP address)
- which pages on our site you visit
- the URL of the Web page from which you came to our site
- which software you use to visit our site and its configuration

This type of data is not personally identifiable.

Links to External Websites

The various University Libraries' websites link to Internet sites and services outside the administrative domain of the libraries. Emory University Libraries does not govern the privacy practices of these external sites. Users should read the privacy statements at these sites to determine their practices. When one or more of the Libraries contracts with vendors for access to online content, such as journals and databases, every attempt is made to include user information protections in the license agreement.

Cookies

A "cookie" is a piece of plain text stored on your computer by a web server and used primarily to customize your interaction with the web. Some cookies last only for the duration of the session, while others are persistent and reside on a computer's hard drive until the user deletes them or the computer is refreshed. As a matter of policy, cookies are erased from Emory University Libraries' public computers periodically throughout the year and at the beginning of each term.

Web Analytics

Emory University Libraries use web analysis tools, including Google Analytics, to capture and analyze web statistics. Google Analytics is a cookie-based analytics program that uses cookies to track website activity. The Libraries also maintain local logs of web activity for statistical assessment using Webalyzer and other log analysis tools. These tools, including Google Analytics, typically collect the following information: Network Location; Hostname; web page(s) requested; referring web page; browser used; screen resolution; size of data transferred; date and time. No personal information is stored within cookies. Cookies can be disabled within a browser's preference or option menu. For more information about Google Analytics, see Google Privacy Center - Privacy Policy.

Accessing Personally Identifiable Information for Other Than Library Business

Purposes

The Library shall only permit the inspection, monitoring, or disclosure of personally identifiable information for other than Library business purposes: (i) when required by and consistent with law, University policy, or campus policy; (ii) when formally requested by an authorized office of the University as part of an official security investigation; (iii) when failure to act might result in

EMORY UNIVERSITY LIBRARIES

Policy on the Collection, Use, and Disclosure of Personal Information

<http://web.library.emory.edu/privacy-policy/personal-information.html>

significant bodily harm, significant property loss or damage, loss of significant evidence of one or more violations of law or of University policies, or significant liability to the Library, University, or members of the University community; or (iv) when there is substantiated reason to believe that violations of law or of University or Library policies have taken place or (v) to comply with a subpoena or court order only with the consent and advice of the University's Legal Counsel.

When under the circumstances described above personally identifiable information must be inspected, monitored, or disclosed, the following shall apply:

Authorization: Except in emergency circumstances, such actions must be authorized in advance and in writing by the University Librarian, or by the Director of Library Technology and Digital Strategies. The Library Cabinet will be notified of each authorization made. Authorization shall be limited to the least perusal of content and the least action necessary to resolve the situation.

Emergency Circumstances: In emergency circumstances -- circumstances in which delay might precipitate harm, loss, or liability as described in (iii) above -- the appropriate Library Cabinet member may approve the least perusal of content and the least action necessary to resolve the emergency, immediately and without prior written authorization, but appropriate authorization must then be sought without delay. All members of the Librarians' Council will be notified of the authorization.

Compliance with Law: Actions taken shall be in full compliance with the law and other applicable University and Library policies.

Compliance with a Subpoena or Court Order: Actions shall only be taken with the consent and advice of the University's Legal Counsel.

Privacy Limits

Library Records: Records pertaining to the business of the Library, whether or not created or recorded on Library equipment, are University records subject to disclosure under Georgia Code § 24-9-46 or to comply with a subpoena or court order.

Possession of University Records: Library employees are expected to comply with requests, properly vetted through University policies and procedures, for copies of records in their possession that pertain to the business of the University, or whose disclosure is required to comply with applicable laws, regardless of whether such records reside on University electronic communications resources.

Unavoidable Inspection: During the performance of their duties, personnel who operate and support electronic communications resources periodically need to monitor transmissions or observe certain transactional information to ensure the proper functioning and security of Library systems and services. On these and other occasions, systems personnel might observe personally identifiable information. Except as provided elsewhere in this Policy or by law, they

EMORY UNIVERSITY LIBRARIES

Policy on the Collection, Use, and Disclosure of Personal Information

<http://web.library.emory.edu/privacy-policy/personal-information.html>

are not permitted to seek out such information where not germane to the foregoing purposes, or disclose or otherwise use what they have observed. Such unavoidable inspection of personally identifiable information is limited to the least invasive degree of inspection required to perform such duties. This exception does not exempt systems personnel from the prohibition against disclosure of personal and confidential information.

Except as provided above, systems personnel shall not intentionally search electronic records or transactional information for violations of law or policy. However, they shall report violations discovered inadvertently in the course of their duties to the Emory University Trust Line (www.finadmin.emory.edu/internalaudit/trustline.html).

Back-up Services

Operators of Library electronic systems shall provide information about back-up procedures to users of those systems upon request.

Changes to Our Privacy Policy


The Libraries may change our Privacy Policy at any time by posting revisions on the website. By accessing or using our website, you agree to be bound by all the terms and conditions of our Privacy Policy as posted on the website at the time of your access or use. If you do not agree to the terms of this Privacy Policy or any revised statement, please exit the site immediately.

Contact Information

If you have any questions about our Privacy Policy, please contact the Administration Office of Emory University Library at 404-727-6861.

Notes

1. Personally identifiable information is any information that can be directly or indirectly associated with a known individual. For example, all information contained in personnel, patron, and circulation files is personally identifiable.
 2. Library business refers to activities involved in the provision, maintenance, and management of the Library's systems and services to its patrons and staff. Circulating books and journals, enforcing Library contracts, and troubleshooting problems with the Library's e-mail system are all examples of Library business. Trying to discover who used a Library workstation to issue a harassing message would typically not be Library business, however.
 3. Substantiated reason to believe requires reliable evidence, as distinguished from suspicion, rumor, gossip, or other unreliable evidence.
-


George A Smathers Libraries

Off-Campus Access

[Home](#) » [Privacy Policy](#)

Privacy Policy

Commitment to Privacy

The George A. Smathers Libraries at the University of Florida values each individual's privacy concerning use of library resources and actively seeks to preserve those privacy rights. Although the Libraries make every effort to protect the privacy of user circulation records and computer use, they may be obligated to release such information to law enforcement agents in response to a search warrant, subpoena, or other lawful directive issued in accordance with the Foreign Intelligence Surveillance Act, 50 U.S.C. 1801, et seq., as amended by the USA PATRIOT Act (Public Law 107-56). Under certain circumstances, library staff may be prohibited from informing you that the Libraries received such a request.

The following information explains privacy policies relating to various library services. However, in legal terms, these shall not be construed as a contractual promise, and the Libraries reserve the right to amend policies at any time without notice. Privacy and public records obligations of the Libraries are governed by University policy, pertinent Florida statutes and by any applicable U.S. federal laws.

Use of Public Workstations in the Smathers Libraries

When visiting the Smathers Libraries, users must log on to public workstations with their Gatorlink username or Guest Gatorlink user ID for persons not currently affiliated with the UF. Log-on records may be used to identify who has used a computer during a specific time period.

Individuals are responsible for logging off when their session is finished in order to protect their privacy and to insure that other individuals are not using a library workstation still logged on to someone else.

[Smathers Libraries Computer Use Policy](http://web.uflib.ufl.edu/computeruse.html)
<http://web.uflib.ufl.edu/computeruse.html>

[UF Policy & Standards: Acceptable Use of Computing Resources](http://www.it.ufl.edu/policies/acceptable-use/acceptable-use-policy/) (including Security and Privacy)
<http://www.it.ufl.edu/policies/acceptable-use/acceptable-use-policy/>

Use of the Smathers Libraries' Web Site

The George A. Smathers Libraries Web site is an official Web site of the University of Florida and maintains information gathered over the Internet in accordance with the University Web Privacy Statement (<http://privacy.ufl.edu/privacy-policies-and-procedures/onlineinternet-privacy-statement/>). The Libraries may also collect specific information necessary to carry out its functions and to serve its patrons.

When you connect to the UF Smathers Libraries' Web, we collect information on browser type, operating system, screen resolution and color depth values, Java and Flash support, referring sites, search terms used to reach our Web site, individual Web pages visited on our site, IP address, and the domain from which a you connected to our site. This information is collected in our internal logs as well as the logs of third-party vendors that provide statistical and software support.

Our Web site also contains links to Web sites and licensed databases that are maintained outside of the University of Florida Libraries. The Libraries are not responsible for the privacy practices of these external third-party Web sites, so you should look for any privacy statements they may have posted on their sites. Some of these services provide options for establishing accounts/profiles to take advantage of enhanced services they offer. If you log on to any of these using a personal username/password, be sure to log off to protect your privacy from others using your workstation.

The Libraries also maintain several web-based management tools, such as forms related to renewing books, asking reference questions, requesting recalls, etc. The personally identifiable information collected and stored in the Libraries' computer or other systems will be used only to maintain your library account and communicate with you. It is not made available to any other entity outside the Libraries, except as required by law.

Under Florida law ([§668.6076, F.S.](#)), email addresses are public records. If you do not want your email address released in response to a public records request, do not send electronic mail to the University. Instead, contact the specific office or individual by phone or in writing.

Ask Us!

UNIVERSITY OF FLORIDA LIBRARIES

Privacy Policy

<http://www.uflib.ufl.edu/privacy.html>

In order to protect your privacy in regard to these services, you should always close your Web browser upon completion of your session.

Borrowing UF Libraries' Materials

The Libraries maintain personally identifiable information for library accounts of valid library users. Items charged out are, of course, linked to the individual who currently has them. Upon return of an item to the library, no record that the item has been borrowed by the individual is retained unless the item was returned overdue and resulted in an overdue fine. Records of non-returned or lost items billed to an individual for replacement are also retained for the same administrative and auditing purposes.

Library circulation records are confidential information. Library staff will not give out the name of a person who currently has an item to another library user, and will not release this information to any other entity outside the Libraries, except as required by law. (See "Confidentiality of Circulation Records" below).

Other Library Services

Confidentiality extends to information sought or received, materials consulted, database search records, reference interviews, interlibrary loan records, and other personally identifiable uses of library materials, facilities, or services. As mentioned above, any personally identifiable information collected and stored in the Libraries' computer or other systems will be used only to maintain your library account and communicate with you. It is not made available to any other entity outside the Libraries, except as required by law.

Confidentiality of Circulation Records – Florida Statutes Section 257.261

Circulation records are confidential in accordance with Section 257.261 of the Florida Statutes. The Statutes state:

"All registration and circulation records of every public library, except statistical reports of registration and circulation, are confidential and exempt from the provisions of s. 119.07(1) and from s. 24(a) of Art. I of the State Constitution. Except in accordance with proper judicial order, a person may not make known in any manner any information contained in such records, except as provided in this section. As used in this section, the term "registration records" includes any information that a library requires a patron to provide in order to become eligible to borrow books and other materials, and the term "circulation records" includes all information that identifies the patrons who borrow particular books and other materials. This section does not prohibit any library, or any business operating jointly with the library, from disclosing information to municipal or county law enforcement officials, or to judicial officials, for the purpose of recovering overdue books, documents, films, or other items or materials owned or otherwise belonging to the library. In the case of a public library patron under the age of 16, a public library may only release confidential information relating to the parent or guardian of the person under 16. Any person who violates this section is guilty of a misdemeanor of the second degree, punishable as provided in s. 775.082 or s. 775.083."

[Staff web](#) | [Departments](#) | [Conduct in the library](#) | [Contact us](#) | [Privacy policy](#) | [ADA/Accessibility](#) | [Employment](#) | [Site index](#)

Send suggestions and comments to [the library web manager](#).

© 2004 - 2016 University of Florida George A. Smathers Libraries.

All rights reserved.

[Terms of Use for Electronic Resources and Copyright Information](#)

This page uses Google Analytics - ([Google Privacy Policy](#))



GEORGETOWN UNIVERSITY LIBRARY

Statement on Data Use for Library Assessment Purposes

<https://docs.google.com/document/d/14iUMpFZFLPaLdAdpQGC9M9UgnjdkI2UBYRKGhwt9KXE/edit?usp=sharing>

Statement on Data Use for Library Assessment Purposes

Submitted for approval from the Assessment Steering Committee - November 2016

The Georgetown University Library occasionally gathers data generated by library users for the following purposes:

- Respond to questions, requests, complaints, or other types of user feedback
- Provide individually customized services like faculty office delivery, InterLibrary Loan, or research consultations
- Monitor library use and demand for services
- Support technology use and network security
- Circulate books, equipment, and other library resources
- Request feedback to assess library programs or services

Data can often be helpful for communication and marketing efforts. Direct quotations from library users should only be used when consent has been given by a specific respondent, or when prior notice has been given to anonymous respondents.

The Library is committed to maintaining all data confidentially (see [Confidentiality of Patron Information](#)) and follows [UIS guidelines](#) for data security. Data gathered during an assessment project should, by default, be considered confidential, meaning that the fewest people necessary will have access to the data, including the project team, relevant department head(s), and relevant AUL(s).

During any activity that gathers feedback from users (survey, focus group, etc.) it is possible that the specific performance or behavior of an individual staff member may be referenced by a user, even if the purpose of the assessment is not to assess the staff member's performance. Sensitive data may be modified or redacted before the data set is shared widely, but an original copy of the data set will be maintained, and modified data entries will be noted within the modified data set.

Non-sensitive data sets may be anonymized and stored in a location that is accessible to all library staff members, such as the Staff Wiki or the Data Dashboard. Aggregated data sets and assessment project reports may also be shared with other Georgetown University departments when requested. To ensure workplace continuity and responsible data use, the Chair of the Assessment Steering Committee and the Assessment Librarian will have access to all data sets gathered for assessment purposes via the Library Assessment Box account.

Indiana University Libraries Privacy Policy

LIB-01



About This Policy

Effective Dates:

12-22-2003

Last Updated:

02-01-2012

Responsible University Administrator:

Dean of Indiana University Libraries

Policy Contact:

Carolyn Walters, Executive Assoc. Dean

Indiana University Libraries

cwalters@indiana.edu

Scope

All users of Indiana University Libraries.

Policy Statement

I. Introduction

Privacy is essential to the exercise of free speech, free thought, and free association. The Indiana University (IU) Libraries define the right to privacy as 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 recognized a right of privacy based on the Bill of Rights of the U.S. Constitution. The state of Indiana guarantees privacy in its constitution and statutory law. (See <https://iga.in.gov/legislative/laws/2015/ic/titles/005/articles/014/chapters/003/> or <http://www.ilfonline.org/units/confidentiality/>). IU Libraries' privacy and confidentiality policies are intended to comply with applicable federal, state, and local laws, as well as with any IU policies on privacy, including the Indiana University policy on [Privacy of Electronic Information and Information Technology Resources](#); a set of frequently asked questions to accompany this policy can be found at: <http://protect.iu.edu/cybersecurity/policies/IT07/faq>. In addition, this privacy policy conforms to the requirements of the IU policy on [Web Site Privacy Notices](#).

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 our users' 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." (<http://www.ala.org/advocacy/proethics/codeofethics/codeethics>)

II. Applicability

This privacy notice applies only to the Indiana University (IU) Libraries and explains our practices concerning the collection, use, and disclosure of user information. Users' information collected by the Indiana University Libraries will be used only as outlined in this privacy notice.

Other units at the University may collect and use visitor information in different ways. Therefore, visitors to other University web sites and those who interact with University units and departments should review the privacy notices for those units or for the particular University web sites they visit. The IU Libraries are not responsible for the content of other web sites or for the privacy practices of University units or web sites outside the scope of this notice.

III. Indiana University Libraries' Commitment to Our Users' Rights of Privacy and Confidentiality

This privacy policy explains our users' privacy and confidentiality rights, the steps the IU Libraries take to respect and protect privacy, and how we deal with personally identifiable information that we may collect from our users.

1. Notice & Openness

The IU Libraries 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.

The IU Libraries post publicly and acknowledge openly the privacy and information-gathering policies of the IU Libraries. Whenever policies change, notice of those changes is made publicly available. In all cases involving personally identifiable information, it is our policy to avoid creating unnecessary records; to avoid retaining records not needed for the fulfillment of the mission of the library; and to avoid engaging in practices that might place sensitive information on public view.

Information that the IU Libraries may gather and retain about current and valid library users includes, but is not limited to, the following:

Circulation Information

This includes all information that identifies a user as borrowing specific materials, including reserve materials.

Collection Development and Resource Management

This includes information regarding the request, purchase, transfer, and related collection management requests linked to individual users or groups of users (e.g., departments).

Electronic Access Information

This includes all information that identifies a user as accessing specific electronic resources, whether library subscription resources, electronic reserves, or other Web resources.

Interlibrary Loan/Document Delivery

This includes all information that identifies a user as requesting specific materials.

Library Surveys/Assessment Projects

This includes any information or data obtained by any IU library through surveys (group or individual interviews or other means) in support of assessment of services, collections, facilities, resources, etc., or in support of research related to library and information services. Any data collected in the course of research is subject to additional review of privacy and confidentiality protections.

Reference/Research Consultations

This includes any information regarding the identity of library users, the nature of their inquiry, and the resources that they consult.

User Registration Information

This includes any information the library requires users (faculty, staff, students, or others) to provide in order to become eligible to access or borrow materials. Such information includes addresses, telephone numbers, and identification numbers.

Other Information Required to Provide Library Services

This includes any identifying information obtained to provide library services not previously listed.

2. Choice & Consent

INDIANA UNIVERSITY BLOOMINGTON LIBRARIES

Privacy Policy

<https://policies.iu.edu/policies/lib-01-libraries-privacy/index.html>

This policy explains our information practices and the choices users can make about the way the IU Libraries collect and use this information.

To provide borrowing privileges, we must obtain certain information about our users in order to provide them with a library account. If users are affiliated with Indiana University, the library automatically receives personally identifiable information (name, address, e-mail address, status [as student, faculty, staff], identification number, etc.) in order to create and update their library account from the Registrar's Office (for students) or Human Resources (for employees). When visiting our library's web site and using our electronic services, users may choose to provide their name, e-mail address, library card barcode, phone number or home address. Users who are not affiliated with Indiana University have the option of providing us with their e-mail address for the purpose of notifying them about their library account. Users may request that we remove their email address from their record at any time.

The IU Libraries never use or share the personally identifiable information provided to us in ways unrelated to the ones described above without also providing users an opportunity to prohibit such unrelated uses, unless we are compelled to do so under the law. Our goal is to collect and retain only the information we need to provide library-related services. The IU Libraries strive to keep all personally identifiable information confidential and do not sell, license, or disclose personal information without consent unless compelled to do so under the law or as necessary to protect library resources or conduct necessary library operations.

3. Access by Users

We attempt to fulfill all requests made by individuals who use library services that require the provision of personally identifiable information and to update their information through proper channels. Users may be asked to provide some sort of verification (e.g., PIN number, photo or network identification card, etc.) to ensure verification of identity.

4. Data Integrity & Security

The data we collect and maintain at the library must be accurate and secure. Although no method can guarantee the complete security of data, we take steps to protect the privacy and accuracy of user data in the following ways:

Data Integrity: We take reasonable steps to assure data integrity, including: using only reputable sources of data; providing our users access to their 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 regularly review and purge personally identifiable information once it is no longer needed to manage library services. Information that is regularly reviewed for purging includes, but is not limited to, personally identifiable information on library resource use, material circulation history, and security/surveillance tapes and logs.

The IU Libraries are committed to investing in appropriate technology to protect the security of personally identifiable information while it is in the library's custody. The IU Libraries follow University policy for the retention of data, and access to data is restricted to a small number of authorized university computing personnel. The IU Libraries post announcements about the choice users make in signing up for customized or personalized services related to web and database services.

Services that Require User Login: In-library computers allow guest use of most library resources without logging in. Use of the full resources of the World Wide Web and of the full power of some subscription databases requires that a user log on to the workstation, either with his/her network ID and password or with a special guest account the user obtains from the library. Data about which users were connected to which machine is collected, in accordance with University policy, and kept for a limited time with very limited access by staff. Users of electronic resources that require authorization for their use are also asked to log in when they connect from outside the university IP address ranges. The data kept from these transactions does not include information linking the user to the resources to which the user connected or about searches completed and records viewed.

Cookies: Cookies are used by IUCAT to maintain the persistence of a default library search limit. These cookies are session cookies and are removed when the user exits the catalog and closes the browser.

Some licensed databases also use cookies to remember information and provide services while the user is online. Users must have cookies enabled to use these resources.

IU Libraries' web sites provide links to other, non-university sites. Indiana University is not responsible for the availability, content, or privacy practices of those sites. Non-university web sites are not bound by this privacy policy and may or may not have their own privacy policies. We are, however, committed to working with vendors of library resources to find solutions that respect the user's privacy and we include a review of the privacy policy espoused by the vendor in purchasing decisions. We provide users with information about the risks of providing personally identifiable information so that they can make reasonable choices about use of personalized services from vendors of electronic library materials. 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, and other use records from library computers and networks.

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 prohibit those individuals with access from utilizing 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. The IU Libraries will not disclose any personal data collected from users to any other party except where required by law, to report a suspected violation of law or University policy, or to fulfill an individual user's service request. We do not sell or lease users' personal information to commercial enterprises, organizations or individuals.

5. Children

This site is not directed to children under 13 years of age, does not sell products or services intended for purchase by children, and does not knowingly collect or store any personal information, even in aggregate, about children under the age of 13. We encourage parents and teachers to be involved in children's Internet explorations. It is particularly important for parents to guide their children when they are asked to provide personal information online.

6. Use of Third Party Analytics Software

Web site developers and owners review usage data on their web pages to identify resources that are being used and to evaluate the provision of information on the site and the effectiveness of the organization and design of that information. This usage data is provided by traditional packaged software and by third-party services. The IU Libraries only use third party analytics software from reputable organizations that have strong privacy policies. Web sites provided by the IU Libraries may use Google Analytics, a web analytics service provided by Google, Inc. ("Google"). Google Analytics uses "cookies", which are text files placed on your computer, to help the website analyze how users use the site. The information generated by the cookie about your use of the website (including your IP address) will be transmitted to and stored by Google on servers in the United States. Google will use this information for the purpose of evaluating your use of the website, compiling reports on website activity for website operators and providing other services relating to website activity and internet usage. Google may also transfer this information to third parties where required to do so by law, or where such third parties process the information on Google's behalf. Google will not associate your IP address with any other data held by Google. You may refuse the use of cookies by selecting the appropriate settings on your browser; however please note that if you do this you may not be able to use the full functionality of IU Libraries websites and linked electronic resources. IU Libraries that use data from Google Analytics and other third-party software providers use such data in the aggregate and do not associate use of any web page or any resource with a particular computer or a particular user.

By using IU Libraries' websites, you consent to the processing of data about you by Google and other providers of usage data in the manner and for the purposes set out above.

INDIANA UNIVERSITY BLOOMINGTON LIBRARIES

Privacy Policy

<https://policies.iu.edu/policies/lib-01-libraries-privacy/index.html>

7. Enforcement & Redress

The IU Libraries will not make library records available to any agency of state, federal, or local government unless required to do so under law or to report a suspected violation of the law. Nor will we share data on individuals with other parties including faculty, staff (including library staff except in the performance of their assigned duties), parents, students, campus security, and law enforcement personnel, except as required by law or University policy or as needed to perform our University duties.

Library staff are to refer all requests for confidential user records to the appropriate Library Dean or Director or their designate. Only the Library Dean/Director or designate has authorization to receive and respond to requests from law enforcement or other third parties. The Dean/Director will forward all requests from law enforcement or other government officials, all requests under applicable "open records" laws, to University Counsel, and will consult with counsel regarding the proper response. Each library within Indiana University will develop written procedures to comply with this policy.

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 complaints about the library's handling of their personally identifiable data should file written comments with the director of the library in question. We will respond in a timely manner and may conduct a privacy investigation or review our policy and procedures. If you feel that the IU Libraries are not following this stated policy and communicating with the Libraries does not resolve the matter, or if you have general questions or concerns about privacy at Indiana University, please contact the University Chief Privacy Officer, 812-855-8476 or privacy@iu.edu.

History

This policy went into effect on December 22, 2003 and was last revised on February 1, 2012.

The latest revision was approved by University Counsel (2/13/2012) and the Council of Head Librarians (2/17/2012).

Related Information

[IT-07, Privacy of Electronic Information and Information Technology Resources](#)

[IT-07, FAQ](#)

[ISPP-24, Web Site Privacy Notices](#)

[Indiana Code 5-14-3, Access to Public Records](#)

[Indiana Library Federation, Confidentiality of Library Records State of Indiana](#)

UNIVERSITY OF MARYLAND



Today: **McKeldin** 08:00AM - 10:00PM

[Home](#) / [About](#) / [Privacy Information](#)

Privacy Information

Introduction

The UMD Libraries respects the privacy of library users in accordance with the American Library Association's document *Privacy: An Interpretation of the Library Bill of Rights*

"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."

Although the University of Maryland Libraries make every effort to protect the privacy of user circulation records (including books and Internet searches), the Libraries and the Division of Information Technology (DIT) with respect to the use of public Libraries work stations may be obligated to release such information to law enforcement agents in response to a search warrant or subpoena, such as those issued in accordance with the Foreign Intelligence Surveillance Act, 50 U.S.C. 1861, as amended by the **USA PATRIOT Act (Public Law 107-56)**. That law prohibits library staff from informing you that it received such a request.

Information We Collect and How it is Used

The user information collected by the Libraries is necessary to provide the requested library services (e.g. book or article delivery), to transfer a reference query to a third party, to comply with license agreements to limit certain electronic resources to the UMD community, and to evaluate and assess our chat and email reference services. Individual server use is not made public.

The following services may require the patron to submit personal information: Aleph - online catalog; e-mail / web forms (e.g., *Ask a Librarian*) and off-campus access to restricted resources (e.g., licensed databases accessed through *Database Finder*, interlibrary loan). Three categories of personal information are collected:

- *Data that are automatically collected* due to Information Technology systems include your browser type, and the domain and Internet Protocol (IP) address from which and to which you are connecting; the source and destination network ports; the date and time of your visit to the site, and the number of bytes transmitted. URLs are not captured. OIT retains login/logout data for up to 8 weeks and Internet transaction data for up to 4 weeks.
- *Data that are collected at the user's request* to customize library services

include personalized settings, such as search preferences on the catalog or in *Database Finder*, marked items, and saved searches.

- *Data that are collected in the course of the day-to-day business* of circulating materials and providing online reference services include your UMD ID number, address, phone number, e-mail address, circulation record, and service requests (e.g., interlibrary loan and reference question).

Circulation records that the University Libraries maintain that contain personally identifiable information about an individual and his/her use of University Libraries facilities may not be inspected or disclosed under the Maryland Public Records Act except by personnel to perform typical Library business. They may be released in response to a search warrant, subpoena or other legal process.

Cookies

Cookies are small pieces of data sent by a Web server and stored by the Web browser. Cookies are used to remember information about preferences and pages visited. For example, if a user's name and password were stored as a cookie, it would save that person from entering the same information when accessing the same service subsequent times during the same browser session. Our website utilizes Google Analytics, a service which uses cookies to collect non-personally identifiable information about website usage (see the **Google Analytics privacy policy** for more information). This data is aggregated and delivered to the Libraries so that we can improve the function and content of our website. Data typically collected include browser used; web pages requested; referring web page; Network Location; screen resolution; date and time. One can refuse to accept or disable cookies by adjusting the browser's settings.

Security

UMD Libraries are committed to keeping personally identifiable information that is required to provide services for the shortest amount of time necessary to complete and manage library transactions. Access to personal information is limited to library staff who need it to provide library services.

Our website contains links to external websites and licensed databases. The University Libraries are not responsible for the privacy practices, security, or content of these external websites. We recommend that you familiarize yourself with the privacy and security information for any site you visit. While we do whatever we can to protect your privacy, please be aware that information or files transferred via the Internet or stored on Internet-accessible computers may be vulnerable to unscrupulous users. Just as in the investing world, you must protect yourself, please be careful and responsible whenever you are online.

Questions?

If you have questions or comments about the UMD Libraries privacy policies and procedures, please contact:

Public Services Division Office, McKeldin Library, Room 4119, University of

[Penn State University Libraries \(/\)](#)

[MENU](#)

[Pattee and Paterno](#) · [7:45 am to 9:00 pm](#) ([/hours-and-locations](#))

Policy UL-AD08 Confidentiality and Privacy of Patron Library Records

Main Policy Content

Contents:

- Purpose
- Introduction
- University Libraries' Policies
 - Library Records
 - E-Mail and Internet
- Applicability and Guidelines
- Family Educational Rights and Privacy Act (FERPA)
- Cross References

PURPOSE:

This document codifies the policies of University Libraries regarding privacy of users' records.

INTRODUCTION:

It is the policy of the Pennsylvania State University Libraries that the privacy of all users, including employees, shall be respected in compliance with federal and state laws and professional standards of confidentiality. This policy applies to all resources regardless of their format or means of delivery as well as to all services offered by the Libraries. We maintain strict client confidentiality and will not reveal the identities of individual users or reveal what information resources they consult or services provided to them to any non-Libraries staff, individual, or entity without a court order or a valid subpoena, or under appropriate federal law.

The University Libraries comply with the [American Library Association's Code of Ethics \(http://www.ala.org/ala/issuesadvocacy/proethics/codeofethics/codeethics.cfm\)](http://www.ala.org/ala/issuesadvocacy/proethics/codeofethics/codeethics.cfm) that 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.

(June 28, 1995)

We also adhere to the Pennsylvania Statute covering the confidentiality of library records that states:

Library circulation records:

Records related to the circulation of library materials which contain the names or other personally identifying details regarding the users of the State Library or any local library which is established or maintained under any law of the Commonwealth or the library of any university, college or educational institution chartered by the Commonwealth or the library of any public school or branch reading room, deposit station or agency operated in connection therewith, shall be confidential and shall not be made available to anyone except by a court order in a criminal proceeding. ([24 P.S. § 9375, 2012 \(http://www.legis.state.pa.us/cfdocs/legis/li/consCheck.cfm?txtType=HTM&ttl=24&div=00.&chpt=000.§n=000.&subsectn=000.\)](http://www.legis.state.pa.us/cfdocs/legis/li/consCheck.cfm?txtType=HTM&ttl=24&div=00.&chpt=000.§n=000.&subsectn=000.))

Many of the University Libraries' records may also be protected under the Family Educational Rights and Privacy Act (FERPA). [See section on FERPA (<https://www.libraries.psu.edu/policies/ul-ad08#ferpa>)]

UNIVERSITY LIBRARIES POLICIES:

PENNSYLVANIA STATE UNIVERSITY LIBRARIES

Policy UL-AD08 Confidentiality and Privacy of Patron Library Records

<https://libraries.psu.edu/policies/ul-ad08>

Library Records:

Records of the borrowing and use of library materials and equipment are considered to be confidential, as are the records of patron transactions of any type including, but not limited to, reference interactions, computer use logs, logs of Internet sites consulted, etc., as well as records of transactions regarding fees and fines. For library purposes, this covers all records related to the circulation or use of laptop computers, camcorders, digital cameras, and any other equipment loaned by the University Libraries as well as books, periodicals, and other formats of printed or electronic information available from the Libraries, including materials that are personally owned by a faculty member that have been placed on reserve for reading in a course. Reference or other service transactions, whether conducted in person, in writing, by telephone, via electronic mail or online interaction, are also considered confidential. Information will be disclosed to law enforcement officials upon request by court order or valid subpoena, or in compliance with appropriate federal law without prior notice.

E-mail and Internet:

E-mail and Internet connections are provided to assist and facilitate library communications. All user files and logs of user transactions on the University and Libraries' systems are held to be confidential and will be kept as private as possible. Collection and analysis of data on usage of the licensed commercial online databases and materials offered by the Libraries through its system assists both the publisher and the University Libraries to understand the impact of this technology and service. We request that any such usage data compiled by the licensor will be collected by a method consistent with applicable privacy laws and written confidentiality requirements of the licensing agreement. Any usage data available, such as number of searches or articles downloaded, is reported at least quarterly by the licensor to the University and is confidential under this policy. Information will be disclosed to law enforcement officials upon request by court order or valid subpoena or under appropriate federal law without prior notice.

The University and Libraries reserve the right to inspect, view and access all data files, electronic messages, and logs of Internet sites consulted by any individuals if it is suspected that the system has been used outside of acceptable use as defined by University policy AD96 Acceptable Use of University Information Resources.

[direct quote from AD96 section II. PRINCIPLES OF ACCEPTABLE USE:]

All individuals' granted access to Penn State information technology resources must agree to and accept the following:

- Using only the information technology resources for which they are authorized by the University.
- Utilizing appropriate authentication mechanisms to access information technology resources.
- Not attempting to access information technology resources for which their authorization may be erroneous or inadvertent.
- Only using accounts, passwords, and/or authentication credentials that have been authorized to use consistent with their role at Penn State.
- Protecting, and not sharing, their account, password, and/or authentication credentials.
- Only sharing data with others as defined by applicable policies and procedures, and dependent on their assigned role.
- Not using Penn State information technology resources to represent the interests of any non-University group or organization unless authorized by an appropriate University department or office or that could be taken to represent Penn State.
- Not using any hardware or software designed to assess or weaken security strength, unless authorized by the institutional CISO or his or her designee(s).
- Not engaging in disruptive "spamming" (i.e., sending unsolicited electronic communication to groups of recipients at the same time), or acting in a way that will harm, damage, corrupt, or impede authorized access to information resources, systems, networks, equipment, and/or data.
- Not forging identities or sending anonymous messages, unless the recipient has agreed to receive anonymous messages.
- Not using Penn State information technology resources to alter, disrupt, or damage information technology resources of another person or entity.
- Not using Penn State information technology resources to upload, download or distribute copyrighted or illegal material which results in violation of law.
- Complying with all licenses and contracts related to information technology systems which are owned, leased, or subscribed to by Penn State, and complying with applicable local, state or federal laws, and institutional policies, rules, and guidelines as they relate to information technology resources.

PENNSYLVANIA STATE UNIVERSITY LIBRARIES

Policy UL-AD08 Confidentiality and Privacy of Patron Library Records

<https://libraries.psu.edu/policies/ul-ad08>

In the event of suspected misuse of Libraries' computational services, the Libraries will act in accordance with the University's Office of Information Security, and in accordance with University policies [AD96 Acceptable Use of University Information Resources](https://policies.psu.edu/policies/ad96) (<https://policies.psu.edu/policies/ad96>) and [AD95 – Information and Assurance and IT Security](https://policies.psu.edu/policies/ad95) (<https://policies.psu.edu/policies/ad95>) (Formerly AD20 Computer and Network Security).

APPLICABILITY AND GUIDELINES:

Any request for patron information that library staff may receive from a law enforcement official should be referred directly to the Dean's office, 510 Paterno Library, University Park, (814) 863-4723.

All Libraries staff and faculty must follow the procedures contained in the Staff Guidelines on Protecting the Confidentiality and Privacy of Patron Library Records [UL-ADG04 (<https://www.libraries.psu.edu/policies/ul-adg04>)]. This applies to all requests for information regarding our library users as well as an individual's library records, etc. This applies to all University Library locations and offices during all hours of service.

FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT (FERPA):

The Family Educational Rights and Privacy Act (also known as FERPA) protects the privacy of students' educational records, including student library financial records. Pursuant to University Policy [AD11](http://guru.psu.edu/policies/AD11.html) (<http://guru.psu.edu/policies/AD11.html>) on Confidentiality of Student Records, the University Libraries ensure compliance with FERPA by not disclosing information about a student's record to any third party, including parents, personnel in an academic department, or other individuals.

Unless there is prior written approval allowing disclosure, the parent (or third party) should be referred back to the account holder (the student) for an explanation. The most frequent inquiry made by parents is about students' library fees that appear on their Bursar Account Statements.

Libraries personnel will annotate the note field in the student's circulation record with a reference to the form on file and refer inquiries to the Libraries' Business Office. Forms will be maintained for no more than three years after the student signature has been affixed.

When there is no form on file, inquiries must be referred back to the student.

CROSS REFERENCES:

Guideline [UL-ADG04](https://www.libraries.psu.edu/policies/ul-adg04) (<https://www.libraries.psu.edu/policies/ul-adg04>) Staff Guidelines on Protecting the Confidentiality and Privacy of Patron Library Records

Effective Date: October 3, 2003

Date Approved: October 3, 2003 (Dean's Library Council; University Legal Counsel)

Revision History (and effective dates):

- December 2017 – Revised to make the E-mail and Internet section current
- August 31, 2015 – Editorial revisions
- March 17, 2008 – Addition of section on FERPA
- October 3, 2003 – Supersedes January 2002 policy
- January 14, 2002 – New policy

Last Review Date: September 2010



[PennState \(http://www.psu.edu\)](http://www.psu.edu)

CONNECT WITH PENN STATE UNIVERSITY LIBRARIES

[Facebook \(/www.facebook.com/psulibs\)](https://www.facebook.com/psulibs)

[Twitter \(/twitter.com/psulibs\)](https://twitter.com/psulibs)

[Instagram \(/www.instagram.com/psulibs/\)](https://www.instagram.com/psulibs/)

PENN STATE
UNIVERSITY LIBRARIES

Syracuse University Libraries

PRIVACY POLICY

Introduction

The Syracuse University Libraries ("Libraries") are committed to protecting the privacy of all who use their services, in person or online. This Privacy Policy provides information about the information the Libraries collect and use, and why they use such information.

The Libraries provide a vast array of services. Many services do not require users to divulge any information to Libraries staff or systems. Other services, however, require users to provide some information in order to receive or benefit from the service.

At all times, the Libraries' staff keeps confidential all information about our users, their activities, and their research choices to the extent allowed by law. All Libraries divisions and personnel comply with New York State law that governs the confidentiality of library records.

The remainder of this Privacy Policy provides details about the Libraries' collection and use of various types of information. If you have any questions, comments, or concerns about this policy, please contact the Director of the Copyright & Information Policy Office at cipa@syr.edu.

Definitions

"Individual Information" includes personal name, physical addresses (including permanent and temporary residence addresses), electronic addresses (including e-mail, instant messaging addresses or screen names, and VOIP addresses or screen names), telephone numbers, and social security number.

"University Information" includes SU ID number, NetID, and any cards or items that include such numbers or identifiers.

"Authenticated Services" are Web-based services the Libraries provide through the Libraries website that require proof that the visitor using the service is affiliated with the Syracuse University community. Authenticated Services – such as "Request," "My Account," "My Bookbag," and using databases off campus – may require users to provide University information.

The **"Libraries Website"** includes content, files, and servers the Libraries manage or control, including, but not limited to, those under the addresses <http://library.syr.edu>; <http://summit.syr.edu>; <http://syracuse.summon.serialssolutions.com/>; <http://copyright.syr.edu>; and associated or successor websites or portals that manage, display or provide information about the Libraries' collections or holdings.

Libraries Privacy Policy (Version 2.0)
Updated October 4, 2013

“Business Transactions” are agreements between individuals or institutions and the Libraries that may have federal or state income tax, trust, or estate implications.

New York State Law

New York State law (N.Y. C.P.L.R. § 4509), which outlines the confidentiality of patron records, says in substantive part:

Library records, which contain names or other personally identifying details regarding the users of ... college and university ... shall be confidential and shall not be disclosed except that such records may be disclosed to the extent necessary for the proper operation of such library and shall be disclosed upon request or consent of the user or pursuant to subpoena, court order or where otherwise required by statute.

“Library records” include information related to:

- » circulation of library materials;
- » computer database searches;
- » interlibrary loan transactions;
- » reference queries;
- » requests for photocopies of library materials;
- » title reserve requests; or
- » the use of audio-visual materials, films or records.

The Libraries and their staff comply with New York’s law concerning the confidentiality of patron records.

Details on Libraries’ Information Gathering

The Libraries perform many functions for the University community. This section provides details about the Libraries’ information gathering practices with respect to each service the Libraries provide to patrons.

1. **Browsing the Libraries website:** The Libraries collect and store certain information automatically when people browse the Libraries’ website. This information includes:
 - Internet domain (e.g., .edu for educational accounts, .com for commercial accounts);
 - IP address;
 - type of browser and operating system used;
 - date and time of access;
 - pages visited; and
 - referring URL.

The Libraries use this information to track site usage, monitor site performance, and generate aggregate statistics. The Libraries, however, do not record, maintain, or track any Individual Information or University Information while visitors are browsing portions of the Libraries website that do not contain Authenticated Services.

2. **Reference:** When visitors seek assistance at the reference desk, the Libraries do not require them to provide Individual Information or University Information. The Libraries may require a visitor to provide University Information, however, in order to use the Libraries' online resources. Also, the Libraries may ask users for Individual Information or University Information in order to improve or customize online or face-to-face reference services.

The Libraries may use information they collect during reference transactions for internal business purposes and to improve the Libraries' services. Whenever this occurs, the Libraries will use the information in a way that eliminates all Individual Information, and strips any personally identifying connectors from University Information.

3. **Classic Catalog:** When users browse or search the [Classic Catalog](#), the Libraries' online public access catalog, the Libraries collect and store information that is similar to what they collect when visitors browse the Libraries website. If visitors seek to use Authenticated Services within the Classic Catalog, however, they must provide University Information.

The Libraries may use information they collect from the Classic Catalog system for internal business purposes and to improve Libraries services. Whenever this occurs, the Libraries will use the information in a way that eliminates all Individual Information, and strips any personally identifying connectors from University Information.

4. **Circulation:** The Libraries require all users to provide University Information in order to borrow materials from the Libraries, including books and laptop computers.

The Libraries may use circulation information they collect for internal business purposes and to improve Libraries services. Whenever this occurs, the Libraries will use the information in a way that eliminates all Individual Information, and strips any personally identifying connectors from University Information.

5. **Interlibrary Loan:** The Libraries require all users to provide University Information in order to borrow materials from other libraries through the inter-library loan ("ILL") service.

The Libraries may use ILL information they collect for internal business purposes and to improve the Libraries' services. Whenever this occurs, the Libraries will use the information in a way that eliminates all Individual Information, and strips any personally identifying connectors from University Information.

6. **Online Resources:** When a member of the University community is on campus, that person can access the Libraries' online resources without having to provide Individual Information or University Information. (This presumes a person already has logged on to the University network, which requires providing University Information.)

When a member of the University community is off campus, however, that person will be required to provide University Information in order to use the Libraries' online databases.

The Libraries may use information that they collect about online database use for internal business purposes and to improve the Libraries services. Whenever this occurs, the Libraries will use the information in a way that eliminates all Individual Information, and strips any personally identifying connectors from University Information.

7. **Technology Loan:** The Libraries require all users to provide University Information in order to borrow technology items.
The Libraries may use University Information and associated data loan information if users fail to return the items as required by the Libraries Technology Support & Loan Policy. Whenever this occurs, the Libraries will provide University Information to the Syracuse University Bursar or the Syracuse University Department of Public Safety. The Libraries will also enable tracking software installed on the technology items to identify their location; tracking may include the use of cameras.
8. **Libraries Research Initiatives:** In order to improve their service to the community, the Libraries occasionally may conduct survey studies, issue questionnaires, or perform other data gathering activities. During these initiatives, the Libraries may ask visitors to provide Individual Information or University Information. In these circumstances, the Libraries consider this information optional; the visitor or user can choose whether or not to provide this information. Further, a visitor's decision to withhold Individual Information or University Information from a Libraries employee who is conducting a research initiative will not harm, diminish, or otherwise affect the level of service that visitor receives from the Libraries.

The Libraries may use information that they collect from research initiatives for internal business purposes and to improve the Libraries' services. Whenever this occurs, the Libraries will use the information in a way that eliminates all Individual Information, and strips any personally identifying connectors from University Information.

9. **Business Transactions:** Under federal or state law, the Libraries may be required to collect, track, and keep Individual Information whenever they conduct a Business Transaction with an individual or institution. In these cases, Individual Information may include taxpayer identification numbers.

The Libraries may use information that they collect from Business Transactions for internal business purposes only. Whenever this occurs, the Libraries will divulge Individual Information only to the following parties:

- University officials who are authorized to handle such information;
- state or federal taxing agencies upon official, written request;
- an individual's duly authorized attorney or estate executor; and/or
- an organization's duly authorized representative, upon written request.

The Libraries retain Individual Information associated with Business Transactions for a period of time mandated by state or federal tax laws, and consistent with the University's data retention schedule.

Summary

This chart summarizes the Libraries' information gathering practices.

Service	Service Type	Individual Information Required?	University Information Required?
Web site browsing	Browsing only	No	No
Web site browsing	Authenticated services ¹	No	Yes
Reference ²	In-Person	No	No
Reference ²	Online	Optional	Yes
Catalog (SUMMIT)	Browsing only	No	No
Catalog (SUMMIT)	Authenticated services ¹	No	Yes
Circulation	All	No	Yes
Inter-Library Loan	All	Yes	Yes
Online Databases ³	On-campus	No	Maybe
Online Databases ³	Off-campus	No	Yes
Technology Loan	All	Yes	Yes
Library Research Initiatives	All	Optional	Optional
Business transactions ⁴	All	Yes	No

Notes:

¹Authenticated services often require University Identification. Includes consultations with the Copyright & Information Policy Adviser.

²On-campus, wireless use of online databases presumes prior authentication to the University network (including AirOrange).

³University Information is required to login from a Library computer workstation.

⁴Federal regulations may require taxpayer identification numbers for certain Business Transactions (including selling books to the Library).

Social Security Numbers

There is no service the Libraries provide - in person or online - that requires a user to provide his or her social security number. Except for Business Transactions, if a Libraries staff member or affiliated Libraries service (including an online database) requests your social security number, please contact the Director of the Libraries' Copyright & Information Policy Office immediately at cipa@syr.edu.

Personal Security

Users share in the responsibility for ensuring that their personal information is adequately protected. It is users' responsibility to protect their University Information. When using the Libraries' computers, users must keep their University Information secure from unauthorized access by keeping their password secret. Users must never leave the Libraries' computers unattended while logged in using University Information. Users must always log out of the Libraries' computers if stepping away from the Libraries' computers.

Links to Other Websites

The Libraries' websites may contain links to other websites of interest. Once users visit such other sites, the Libraries cannot control the protection and privacy of any information users provide on those other sites. Users should exercise caution and look at the privacy statement applicable to the website in question.

Contact


If you have any questions about this Privacy Policy, please contact us through our website or write to the Libraries at:

Syracuse University Libraries
222 Waverly Avenue
Syracuse, New York 13244
Attn: Director, Copyright & Information Policy Office
E-mail: cipa@syr.edu

Metadata

Version: 2.0
Author: Pamela W. McLaughlin
Editors: K. Matthew Dames; Amy Vanderlyke Dygert
Date: August 1, 2009; October 4, 2013
URL: <http://library.syr.edu/policies/privacy.html>
Contact: cipa@syr.edu

Libraries Privacy Policy (Version 2.0)
Updated October 4, 2013



TEMPLE UNIVERSITY®

See hours for all locations | Today's Hours

Samuel L. Paley Library	8:00 am - 7:00 pm
Ambler Campus Library	7:30 am - 5:00 pm

University Libraries

Home

Find

Services

About

Collections

Ask / Help


Home › Ask / Help ›

Ask Us

Sorry, chat is offline but you can still get help.

Email us your question

You may also get help from the [Ask Here PA service](#).



Quick Links

- Ask a Librarian
- Contact Us
- Course Reserves
- Database Finder
- E-ZBorrow
- Find Articles by Citation
- How Do I...?
- ILLiad
- Journal Finder
- Library Search
- RefWorks
- Request Forms
- Research Guides
- Reserve Study Rooms

Ask a Librarian: Privacy Policy

Temple University Libraries respects the rights and privacy of our patrons and their records in accordance with the following institutional and professional policies and state law. Temple University Libraries understands "patron records" to include all records with identifying information about patrons, including the contextual information in transcripts of reference interactions.

- Temple University Computing and Network Security Policy (pdf)
- Pennsylvania Law for the Confidentiality of Library Records (pdf) [PDF]
- ALA Policy on Confidentiality of Library Records

1) What Information is collected by the service?

Email, chat and text transcripts, as well as the IP addresses of users, are logged by a third-party vendor, Springshare (<http://springshare.com>). All transcripts are password protected, for view only by designated library staff. These transcripts are restricted for the purposes of internal training, statistical reporting, and may at times be re-purposed, once stripped of any identifying information, in the FAQ knowledge-base.

Please note that users contacting us through the chat widgets on the library's webpages are anonymous, though you may provide your name if you wish. Any chats occurring through commercial instant message (IM) providers (AIM, Google, Windows Live, Yahoo!) may be logged by those companies. For more information, review the privacy policy of your IM account provider.

2) What is the information used for?

The transcripts are analyzed for the amount and types of questions we are being asked. This helps determine appropriate staffing levels and aids in training librarians to staff the service. Frequently asked questions may be at times be mined and re-purposed in order to populate the FAQ knowledge-base, but no identifying information is made public.

3) Who has access to this information?

The information collected by the library and Springshare is accessible to Temple Libraries' librarians, staff, and administrators who need it in the course of their work.

4) Does the library share the information?

Statistics generated from chats, emails, and texts may be used for official reports or publications of the Temple University Libraries. However, information about specific individuals (e.g. IP address, email address, name, phone number, etc.) will never be shared outside of the Temple University Libraries except as may be required by law.

5) What choices do users have about the collection, use, and distribution of their information?

Any patron may request to have their chat, email, or text transcript deleted by contacting the Libraries' Learning and Research Services department. Users will need to provide their name or email address or phone number, along with the date and approximate time of their transaction in order to help identify the correct transcript for deletion. [Contact jbaldwin@temple.edu, or 215-204-4585]

Last Updated: 01/25/2018



University Libraries

WU Libraries Privacy Statement

Thank you for visiting the Washington University Libraries website and reviewing our privacy policy. Our privacy policy is clear: We will collect no personal information about you when you visit our website unless you choose to provide that information to us, such as by submitting a question, requesting an item, or otherwise 'doing business' with the Libraries.

Although we try to protect the privacy of user records (including books and Internet searches), the Libraries may be obligated to release such information to law enforcement agents in accordance with state or federal law. Unless otherwise precluded by law, the Libraries will inform library users that their records have been accessed. Please see [Confidentiality of Washington University Library Records](#) for more information.

The following discloses the information gathering and dissemination practices of the University Libraries for these websites: library.wustl.edu, catalog.wustl.edu (spokane.wustl.edu), libcat.wustl.edu, illiad.wustl.edu, ares.wustl.edu, orb.wulib.wustl.edu, digital.wustl.edu, and any other servers running publicly-accessible library services.

INFORMATION COLLECTED AND STORED AUTOMATICALLY

If you do nothing during your visit but browse through the website, read pages, or download information, we

WASHINGTON UNIVERSITY IN ST. LOUIS LIBRARIES

WU Libraries Privacy Statement

<https://library.wustl.edu/about/policies/privacy/>

will gather and store certain information about your visit automatically. This information does not identify you personally. We automatically collect and store the information usually logged by web servers: such as Internet domain and IP address; type of browser and operating system used to access our site; date and time you access our site; pages you visit; and if you linked to our website from another website, the address of that website.

We are also implementing Google Analytics to help analyze how users use the site. The tool uses “cookies,” which are text files placed on your computer, to collect standard Internet log information and visitor behavior information in an anonymous form. The information generated by the cookie about your use of the website (including your IP address) is transmitted to Google. This information is then used to evaluate visitors’ use of the website and to compile statistical reports on website activity for Washington University Libraries.

We will never (and will not allow any third party to) use the statistical analytics tool to track or to collect any personally identifiable information of visitors to our site. Google will not associate your IP address with any other data held by Google. Neither we nor Google will link, or seek to link, an IP address with the identity of a computer user. We will not associate any data gathered from this site with any personally identifiable information from any source, unless you explicitly submit that information (see below).

We use this information to help us make our site more useful to our primary users, the current students, faculty, and staff of Washington University.

IF YOU SEND US PERSONAL INFORMATION

If you choose to provide us with personal information as

in an email to one of our online email boxes, or by filling out a form with your personal information and submitting it to us through our website, we use that information to respond to your message and to help us get you the information you have requested. We do not collect personal information from such communications for any purpose other than to respond to you. We do not collect information for commercial marketing.

DOING BUSINESS WITH THE LIBRARIES

In order for current Washington University students, faculty, and staff to 'do business' with the Libraries – that is, check out materials, and access off-campus resources via the proxy server – the Libraries maintain a patron database. Your record in this database contains your name; address; phone number; WUSTL Key username; University ID number; a designator that indicates whether you are a student, faculty, or staff member; and your email address. It also contains information as to which items you have currently checked out, and if you owe any fines. The Libraries use the information in your patron record *only* to allow you to 'do business' with us.

We also keep information about you if you use ILLiad (Interlibrary Loan), on illiad.wustl.edu. Your record in this database contains your name; address; phone number; University ID number; your status with the University (student, faculty, or staff); your email address; and your WUSTL key. It also contains information about the ILL requests you have made, including the status on each request. Again, the Libraries use the information in your ILLiad record *only* to allow you to 'do business' with us.

If you are an instructor using Ares (electronic reserves), you have an account that contains your name, WUSTL key, email address and sometimes your mailing address. Ares is available only on the University campus or to people with valid library accounts. Your name is shown

on Ares to those who have the password to any of your courses with materials on Ares. You have access to this information using WUSTL key and password. If you do not know your course password, contact the Olin Reserves Unit.

If you login to *Find it!* you are creating a record on *orb.wulib.wustl.edu*. This record, in terms of what authorized library staff can view, contains only your WUSTL key username. You can save citations and your favorite sets of databases, but library staff cannot view this information.

LINKS TO OTHER SITES

This site contains many links to other sites, primarily databases and electronic journals which the Libraries have licensed for the use of Washington University students, faculty, and staff. Washington University Libraries are not responsible for the privacy practices or the content of such websites. Once you link to another site (any URL that does not begin with any of the server names listed above, outside of *.wustl.edu), you are subject to the privacy policy of the new site – which may differ considerably from the Libraries policy.

SITE SECURITY

To guard against unauthorized access, maintain data accuracy, and promote the correct use of information, we have put in place physical, electronic, and managerial procedures to safeguard and secure the information we collect online.

However, while we consider these measures reasonable, no assurance can be given that they will always and in all cases prevent or protect against invalid access or improper activity, and any expectation or warranty of unassailable site security is expressly disclaimed.