Oregon State University Libraries Privacy Policy

Introduction

Oregon State University Libraries (hereafter "OSUL") affirms its commitment to "privacy of inquiry, confidentiality, and no fear of censure or examination" in its statement on Intellectual Freedom. Privacy is essential for free speech, free thought, and free association. OSUL recognizes the possibility of surveillance (whether direct or through access to records of speech or research) of users - undergraduate students, graduate students and faculty, staff, community card holders, and others not accounted for by those statuses - undermines a democratic society. In libraries, the right to privacy includes the right to open inquiry without having the subject of one's interest examined or scrutinized by others. Oregon Revised Statute 192.355 (23) exempts from disclosure under open records law the records of a library, including: (a) circulation records, showing use of specific library material by a named person; (b) the name of a library patron together with the address or telephone number of the patron; and (c) the electronic mail address of a patron.

This document defines how OSUL intends to respect and protect users' privacy when using OSUL resources and services. It addresses how OSUL will handle personally identifiable information that the organization may need to collect from users in order to provide services to meet users' needs. The policy will be reviewed routinely as new technology and practices emerge to ensure OSUL is protecting user privacy. This policy does not cover services provided by other units housed within the Valley Library, such as Student Multimedia Services and the Undergraduate Research and Writing Studio.

Notice and Openness

Some library services necessitate the retention of some information. Library visitors should be aware of the policies governing records and personally identifiable information. If a library program or service requires the retention of this information, all attempts will be made to inform why that is necessary. As an institution, we will avoid retaining records not relevant to the ongoing mission and focus of the library. We will protect user data to the extent possible. Data we may retain about current library users includes, but is not limited to:

- User registration records
- Active circulation records
- Interlibrary loan records
- Electronic access information
- Patron demographic data obtained from central databases maintained by the university
- Information when users login to computers in OSUL's Learning Commons
- Other information required by public services

We also collect the following information when users visit the OSUL website and digital repositories:

- Domain, country, IP address
- Browser, platform (device and operating system), resolution
- Entrance-exit pages, referrals
- Date and time
- Search terms and search engines
- ONID

This is standard practice for web content and information collected is not used for any reason besides evaluating website use and identifying key areas of website development and improvement.

Choice and Consent

In order for users to access some library services, OSUL must use personal information to create a user account. If you are affiliated with Oregon State University, OSUL automatically receives information from other campus systems, such as Banner, to create and update a user's main library account. When visiting the Libraries' electronic services (such as interlibrary loan and library databases), users are asked to provide an ONID username and password. Users may also be asked to provide their university/library account number, phone number, and/or home address.

Access by Users

Some personal and identifiable information collected for OSUL user accounts can be viewed and updated online. Changes to information that is passed from campus systems such as Banner or ONID must be made in those systems. OSUL also creates library accounts for persons within the Corvallis community. These community card users may update all their library account information in person, and they will be asked to provide verification of their identity to do so. It is important for library users to keep personal information up to date to ensure that library operations can function properly. Such functions may include notification of overdue items, recalls, reminders.

Data Retention & Tracking

Data Retention: OSUL continues to protect personal information from unauthorized disclosure once it is no longer needed to manage library services. Information purged or shredded at regular intervals designated by OSUL includes personal information from reference interviews and instruction sessions, and circulation history regarding materials in our library collections. Transcripts from chat reference sessions are stored in a third party system that anonymizes names.

The Libraries' Special Collections and Archives Research Center is mandated to follow a more strict circulation policy. OSUL manages the University Archives which contains permanent historical records about the University as well as Special Collections materials. In the context of managing and providing access to these materials, SCARC adheres to the Society of American Archivists' Core Values Statement and Code of Ethics for Archivists. SCARC maintains a separate database and reference file that contain user registration and circulation information, but this information is confidential.

Security Cameras: The Valley Library maintains and operates a collection of security cameras meant to preserve a safe environment for all visitors to the Valley Library. The Guin Library at Hatfield Marine Science Center in Newport maintains one security camera at the library entrance. Data are recorded and retained for a period of two weeks. Access to the data recorded from these devices is maintained exclusively by select individuals within OSUL and at Guin. Security camera footage may be released to law enforcement if subpoenaed or at the discretion of the University Librarian. Questions about where cameras are located within Valley Library or Guin Library can be addressed to the Valley Library building manager or the director of the Guin Library.

Disclosure of data is addressed in the section on **Disclosure of Personal Data and Usage Data.** More specific information about how long individual records are retained and how users may opt out of sharing personal data is available in the table on pages 5-6 of this document.

Tracking Users: To maximize functionality and access, we ask OSU-affiliated users to use their ONID credentials to log in to online library services. We may require ONID authentication or an OSU ID card for users to borrow materials, request special services, register for programs or classes, or make remote use of those portions of the OSUL website restricted to registered borrowers under license agreements or other special arrangements. Additionally, some library vendors may require users to create accounts to use their online resources or sites; these accounts are not under the OSUL's control. However, we regularly clear cookies, web history, cached files, or other computer and Internet use records and other software code placed by users on our library computers.

Cookies: Users of networked computers will need to enable cookies in order to access a number of resources available through OSUL. A cookie is a small file sent to the browser by a website 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. Users can refuse to accept cookies, can disable cookies, and remove cookies from their hard drives. Our library servers use cookies solely to verify that a person is an authorized user who is allowed access to licensed library resources. We do not share cookies information with external third parties. Some third-party library vendors may use cookies for their sites, but these cookies are not under OSULs' control.

Security Measures: Our security measures involve managerial and technical policies and procedures, and contractual agreements with system vendors to protect against loss and the unauthorized access, destruction, use, or disclosure of user data. Our technical security measures to prevent unauthorized access include encryption in the transmission of data where possible, and storage of data on secure servers or computers. In the case of a data breach, the policies of the Office of Information Security will be followed.

Disclosure of Personal Information and/or Usage Data

OSUL permits only authorized library staff with assigned confidential passwords to access personal data stored in the Libraries' computer systems for the purpose of performing library work. OSUL does not sell or lease users' personal information to companies, universities, or individuals. OSUL will not disclose personal data collected during reference interviews, instruction sessions, or other activities to any other non-library parties. OSUL also will not make library circulation records and other data related to usage of collections, services and facilities available to non-library parties.

Where required, exceptions include:

- system-related needs (i.e., third-party library service providers who have contractually agreed to maintain user confidentiality)
- fulfillment of an individual user's service request;
- compliance with a valid subpoena, warrant, court order, or other investigatory document after the University's General Counsel has determined that the Libraries are required to comply.

Only the University Librarian or designee(s) is authorized to receive and/or comply with requests from law enforcement officers; responses to requests are done in consultation with the OSU Office of General Counsel.

Violations of Policies and Laws Prohibited and Not Protected

Users must comply with established institutional and library policies and with the law while using the Libraries' resources and services. Nothing in this statement prevents the Libraries from performing its duties in relation to: enforcement of established University or library rules or policies; compliance with legal obligations; protection of the Libraries' facilities, network and equipment from harm; or prevention of the use of the Libraries' facilities and equipment for illegal purposes. If evidence would cause a reasonable person to believe that a violation of laws and/or established institutional or library policies has taken place in its facilities or operations, the Libraries reserves the right to electronically monitor its public computers and network, and/or reveal a user's identity to institutional authorities. Staff members are authorized to take immediate action to protect the security of library users, staff, collections, data, facilities, computers, and the network.

Questions about This Policy

Questions about this policy can be directed to the University Librarian. Library users who have questions, concerns, or complaints about the Libraries' handling of their privacy and confidentiality rights may file written comments with Library Administration. The University Librarian will respond in a timely manner and may conduct a privacy investigation or review of policies and procedures.

Statement and Attribution

This privacy policy has been adapted from the University of Oregon Libraries Privacy Statement, which is based on the American Library Association Privacy Policy model. It was reviewed in the 2017-18 academic year by OSUL's Library Faculty Association, Library Administration Management and Planning, and in FY19 by Oregon State University General Counsel.
It became effective October 15, 2019.

Information collection, retention and opt in /opt out details		
Library Services	**Opt in/opt out?**	**Additional Information**
Viewing physical materials in the Special Collections and Archives Research Center. Personally identifiable information for individuals accessing SCARC material is recorded and may be visible to library or security personnel.	Opt out by not using this service. Archivists can work with you to scan the material you need, instead. This information is kept for 5 years.	This is a best practice recommended by the archival/rare book community, so it is not expected to change in the future.
Checking out materials from the library. Currently, our circulation system stores emails that are sent to users regarding recalls, overdue materials, loans, requests and etc.	In May 2017, our system was upgraded to allow for anonymization of notification messages. Please note that anonymization is turned on by default for all users. There will be a period of no more than 7 days that the messages are stored in the system before this process occurs. For long overdue or billed items, notices are retained for up to a year for financial verification purposes. ● Short loan item (e.g. course reserves and equipment) - long overdue at 2 days past due date ● Long loan item (e.g. items from main collection) - long overdue at 42 days past due date	Fines and billing data are required records retention so that questions about patron financial accounts can be accurately answered.
Interlibrary loan. Interlibrary loan usage is governed by the American Library Association Code for the United States. This code requires a retention schedule of interlibrary loan requests for 5 years. Requests contain personally identifiable information and bibliographic information.	Opt-out of this service by not using interlibrary loan. This data is kept for 5 years.	This data is used to see trends in service usage over time, and to provide data for collection development decisions.

Information collection, retention and opt in /opt out details		
Library Services	**Opt in/opt out?**	**Additional Information**
Emails received by the library and library units. Emails received are kept by Information Services. Examples of communications that are stored include messages to interlibrary loan, circulation, or the library information desk about anything library related.	Users can receive direct help from library staff by calling the library directly at (541) 737-3331.	
Chat. When you talk with us through our chat system, a transcript of the discussion, date and time of the discussion, your IP address, and name are all recorded and stored.	Opt out by not using this service. If you have a reference question you'd like to talk to a librarian about, please come into the library or call us.	
Reference. We use a third party tool to manage and study our reference questions. These questions come in from chat, system form inputs, email, texts, and are recorded after in-person sessions. We use this data to better characterize the types of questions we are addressing. Names, if given, may be recorded in this database.	Opt out by not giving your name or email address when using this service.	
1Search. Search queries entered into 1Search are anonymized and stored for analytics purposes.	You may opt-out by not using 1Search for your research needs. Your search query in 1Search is routinely anonymized. Please note that 1Search may redirect to a third-party vendor that may collect user data.	
Third-party vendors and publishers. The Libraries license digital content and databases hosted and administered by third parties and participate in consortia that access some of our data.	Opt out by not using these services.	