South Carolina

University Libraries

Collection, Disclosure, and Use of Personally Identifiable Information

2022

University of South Carolina Libraries
2022

Table of Contents

University of South Carolina Libraries
2022

Introduction

Privacy and confidentiality are fundamental values of libraries and are vital to the preservation of academic freedom. According to the American Library Association, "all people, regardless of origin, age, background, or views, possess a right to privacy and confidentiality in their library use. When users recognize or fear that their privacy or confidentiality is compromised, true freedom of inquiry no longer exists" (ALA, 2006). The University of South Carolina Libraries respects the confidentiality of patron records and communications in all formats in compliance with federal and state law, and with university data privacy policies.

The following policy describes how University Libraries collects and uses the personally identifiable information (PII) of patrons (university-affiliated and guests) while providing library services.

Data Collected by the Libraries

University Libraries collects several types of digital data while providing access to the libraries' physical and electronic resources. Personally identifiable patron data collected by University Libraries falls into several categories:

- **Data provided by the university**. The Libraries obtain student data from the Student Services' Banner system and employee data from Human Resources. These data are regularly loaded into library systems via an automated process to ensure that we are providing members of our user community access to our services and collections.

- **Data provided by the patron**. Examples of data collection points include Carolina Card swipes at library entrance and exit points, book or other materials check outs, requests for access to special collections, email messages to library employees, and messages sent through the library's chat platform.

- **Data generated in the libraries**. The library operates security cameras at points throughout the library. This footage may include images of patrons' faces that would allow other people or machines to identify them. Video footage collected at the library is hosted by and is accessible to UofSC Law Enforcement and Safety and is limited to review by trained UofSC Libraries personnel. Footage is hosted for one year before deletion.

For data collected by the Libraries, internal unit policies will determine procedures for the removal of patron data and records. For example, Special Collections units retain information for perpetuity for the safety and security of the collections.

Some data the libraries collects is not PII. Examples include:

- The user's IP address
- Pages visited on the library website
- Referring URL
- Software used to visit the library website and the configuration of that software.

Data Collection – 3rd Parties

When using library resources, patrons often leave the library website and search databases and websites beyond the domain of the University of South Carolina Libraries. These websites may collect personal information about visitors. Certain sites may also require or suggest registration. A website's collection and use of this information is governed by their own policies rather than those of the UofSC Libraries; however, the Libraries makes every effort to negotiate policies that protect the privacy of our patrons. To learn how data collected by third parties are used, patrons should view the privacy statements that can be found at these sites.

Who Has Access?

Access to Personally Identifiable Information collected by the UofSC Libraries is restricted to trained personnel and used solely for the purpose of providing library services, such as patron access to physical resources, electronic resources, Libraries facilities, and assistance from Libraries personnel.

Sharing Data

The UofSC Libraries shares limited patron data with third parties in order to provide access to certain resources. Whenever possible, data sharing to third parties is restricted to the information that is necessary to authorize patron access to electronic resources.

Personal information on library patrons that is requested by government agencies will not be shared without a subpoena executed by a court of law unless it is deemed essential for an emergency situation as described in Data Privacy Limits.

Data Security

The UofSC Libraries takes steps to ensure that patron data is secure by collecting the minimal amount of Personally Identifiable Information necessary to provide library services. Access to this data is restricted to trained personnel. For assessment and reporting purposes, the Libraries aggregates and strips identifying information.

Data Privacy Limits

Emergencies

The library may permit inspection, monitoring, or disclosure of personally identifiable patron information for reasons other than normal library business only:

- When required by law
- When required by university policy
- When there is a substantial risk that data submitted by a patron to University Libraries systems or third-party vendors is identified as posing potential harm or loss of property to members of the university community (for example, by using a library service platform to share hate speech or threats).

Necessary Inspection

While performing work duties at University Libraries, trained personnel, including circulation and information technology staff, will have unavoidable contact with patron Personally Identifiable Information.

Enforcement

Patrons of the University of South Carolina Libraries who have questions or concerns about patron data privacy should contact the relevant Data Steward.

Only the Dean of UofSC Libraries, who serves as Data Trustee for the unit, is authorized to interact and comply with requests for information from law enforcement. If such a request is received, the Dean will confer with the Office of the President and the University's General Counsel to determine the appropriate response. Library records will not be made available to any law enforcement entity without a subpoena, warrant, or other legal order that has been issued by a judge. University Libraries faculty, staff, and student workers are trained to refer all such law enforcement inquiries to the Libraries Administration.

Your Rights

The UofSC Libraries will ensure that your data is protected to the greatest extent possible. You have the right to request a copy of the data that is collected by the Libraries, and to correct this information if necessary. In some circumstances, we may be able to delete or to further restrict access to this data.

To exercise these rights or to contact us with concerns, comments, or complaints about the University Libraries' handling of patron data, please contact the Dean of UofSC Libraries or the relevant Data Steward in writing. Your request or comments will be reviewed and responded to in a timely manner. We will attempt to fulfil your request to the greatest extent possible but be aware that your request may not be covered under the scope of this policy and that the Libraries may be limited in its ability to delete or restrict access to data collected by third-party vendors.

References

American Library Association. (2006, July 7). *Privacy: An Interpretation of the Library Bill of Rights*. Advocacy, Legislation & Issues. https://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy

MIT Libraries. (2020, November). *MIT Libraries Patron Data Privacy Policy*. https://libraries.mit.edu/about/policies/privacy-policy/

Murray State University Libraries. (n.d.). *Murray State University Libraries Privacy Policy*. Retrieved May 26, 2022, from https://libguides.murraystate.edu/c.php?g=990196&p=7194674

Pacific Library Partnership. (2020, September). *Data Privacy Best Practices Toolkit for Libraries.* https://www.plpinfo.org/wp-content/uploads/2020/10/PLP_Toolkit_Final-Accessibility-Modified.pdf

Rutgers University Libraries. (2010). *Privacy Policy*. https://www.libraries.rutgers.edu/about-rutgers-university-libraries/policies-and-guidelines/privacy-policy

University of California Berkeley Library. (2022, March 7). *Collection, Use, and Disclosure of Electronic Information*. https://web.archive.org/web/20220307210149/https://www.lib.berkeley.edu/about/privacy-electronic-information

University of South Carolina Libraries
2022

University of South Carolina. (n.d.). *Data Stewards.* Retrieved June 3, 2022, from https://www.sc.edu/about/offices_and_divisions/division_of_information_technology/chiefdataofficer/datastewards.php

University of South Carolina (2018, April 9). *Responsible Use of Data, Technology, and User Credentials.* https://sc.edu/about/offices_and_divisions/division_of_information_technology/docs/univ152.dec2021.pdf

University of South Carolina (2019, December 13). *Data and Information Governance*. https://www.sc.edu/policies/ppm/univ151.pdf

University of South Carolina (2022, May 19). Roster of Data Stewards. https://sc.edu/about/offices_and_divisions/division_of_information_technology/chiefdataofficer/datastewardroster.pdf