PROTECTING PATRON PRIVACY

The Scenic Regional Library defines the right to privacy in the library as the right of individuals to lawfully use the library's resources to pursue their inquiries without having the subject of their interest examined or scrutinized by others. Confidentiality exists when the library obtains personally identifiable information about users that is necessary for the operation of the library, and undertakes to keep that information private on their behalf.

The courts have upheld the right to privacy based on the Bill of Rights of the United States Constitution. Many states, including Missouri, provide guarantees of privacy in their constitutions and statutes.

Missouri Revised Statutes 2015 defines the responsibility of the library in safeguarding personally identifiable information:

182.817.1 Disclosure of library records not required – exceptions.

1. Notwithstanding the provisions of any other law to the contrary, no library or employee or agent of a library, or third party contracted by a library that receives, transmits, maintains, or stores library records, shall release or disclose a library record or portion of a library record to any person or persons except:

(1) In response to a written request of the person identified in that record, according to procedures and forms giving written consent as determined by the library; or

(2) In response to an order issued by a court of competent jurisdiction upon a finding that the disclosure of such record is necessary to protect the public safety or to prosecute a crime.

2. Any person whose privacy is compromised as a result of an alleged violation of this section may file a written complaint within one hundred eighty days of the alleged violation with the office of the attorney general describing the facts surrounding the alleged violation. Such person may additionally bring a private civil action in the circuit court of the county in which the library is located to recover damages. The court may, in its discretion, award punitive damages and may award to the prevailing party attorney's fees, based on the amount of time reasonably expended, and may provide such equitable relief as it deems necessary or proper. A prevailing respondent may be awarded attorney fees under this subsection only upon a showing that the case is without foundation.

3. Upon receipt of a complaint filed in accordance with subsection 2 of this section, the attorney general shall review each complaint and may initiate legal action if deemed appropriate.

Numerous decisions in case law have defined and extended rights to privacy. The Scenic Regional Library privacy policy and procedures comply with applicable federal, state and local laws.

User rights --- and the library's responsibilities --- as outlined here are based in part on five principles of fair information practice: the rights of Notice, Choice, Access, Security and Enforcement.

Scenic Regional Library's commitment to the privacy and confidentiality of our users also is rooted 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."

COMMITMENT TO USERS' RIGHTS

Notice and Openness

Library users have the right of "notice" --- the right to be informed about policies governing the kind of information the library collects, why the information is necessary to provide library services, how long the library retains the information, and how the library disposes of it.

Such policies are freely available to all library users. Changes or revisions in policies are also available. Scenic Regional Library's Privacy Policy is posted on the library website.

In all cases it is the practice of the Scenic Regional Library to avoid creating unnecessary records of personally identifiable information, to retain such necessary records only as long as they are needed for the operation of the library, and to avoid engaging in practices that might place such information on public view.

Information the library may gather and retain is limited to current and valid library users. Such records include:

- Borrower Registration Information
- Circulation Information
- Electronic Access Information
- Information Required to Provide Library Services, such as Interlibrary Loan, Books by Mail Service, and Program Registrations

Choice and Consent

Other than the personal information necessary to maintain a library account, the library will not collect or retain a patron's personally identifiable information without their consent. If a

patron consents to give the library their information, the library will keep it confidential and will not sell, license or disclose personal information to any third party without the patron's consent, unless the library is compelled to do so under the law or to comply with a court order.

If a patron wishes to receive borrowing privileges, the library must obtain certain information about the individual in order to provide them with a library account. When visiting the library's web site or using the library's electronic services, a patron may choose to provide their library card barcode and personal PIN to access certain services.

A patron has the option of providing the library with their e-mail address for the purpose of notifying them about their library account. A patron may request that the library remove their e-mail address from their account at any time.

The library never uses or shares the personally identifiable information provided to the library in ways unrelated to the ones described above without also providing the patron an opportunity to opt out or prohibit such uses, unless the library is compelled to do so under the law or to comply with a court order.

Access by Users

Individuals are entitled to view the personal information in their library accounts online. Updates may be done in person at the library. If a patron does not have their library card with them, they will be asked to provide some type of photo identification (such as a driver's license) to verify their identity, or be asked to verbally verify information on their account. Updates may be submitted online and are subject to verification. The purpose of updating the personally identifiable information in a patron's account is to ensure that the library can function properly. Such functions may include notifications of overdue items, holds, reminders, and other announcements. The library will explain the process of accessing or updating a patron's information so that all personally identifiable information is accurate and up to date.

Data Integrity and Security

Data Integrity: The information the library collects and maintains must be accurate and secure. Scenic Regional Library shall take reasonable steps to ensure data integrity, including: using only reputable sources of data; providing users access to their own data; updating data whenever possible; utilizing software authentication systems that authorize use without linking it to personally identifiable information; destroying untimely data or converting it to anonymous form.

Data Retention: The library protects personally identifiable information from unauthorized disclosure once it is no longer needed to manage library services. All public computer usage logs are purged after 60 days. Hard copy circulation records (for example, interlibrary loan records) are shredded after materials are returned and/or fines or fees paid in full. Program registration logs are shredded at the conclusion of the program. If the library sets up mailing lists to notify patrons of future programs or events, patrons will have the option to sign up

separately for such mailing lists, and lists will be deleted or shredded when they have been inactive for six months.

Tracking Users: Scenic Regional Library does not ask library visitors or web site visitors to identify themselves or reveal any personal information unless they are borrowing materials, using public access computers, requesting special services, registering for classes or programs, or making remote use from outside the library of those portions of the library's website restricted to registered borrowers under license agreements or other special arrangements.

Third Party Security: The library ensures that all of Scenic Regional Library's contracts, licenses, and offsite computer service arrangements reflect library policies and legal obligations concerning user privacy and confidentiality. Should a third-party vendor require access to Scenic Regional Library users' personally identifiable information, the library's agreements with the vendor shall address appropriate restrictions on the use, aggregation, dissemination and sale of that information, particularly information about minors including obtaining the necessary consent of Scenic Regional Library users.

In circumstances where there is a risk that personally identifiable information may be disclosed, it is the library's obligation to warn users. When connecting to licensed databases outside the library, the library releases only information that authenticates users as "members of our community." Nevertheless, the library advises users of the limits to library privacy protection once they leave the library web site to access remote sites not under the library's control.

Security Measures: The library has security measures in place to protect personally identifiable information while it is in the library's custody, and to ensure that aggregate, summary data is stripped of personal identifiers. Library security measures include both management and technical policies and procedures to protect against loss and the unauthorized access, destruction, use or disclosure of data. Only library employees who need access to data to carry out their library functions are authorized to access that data, and only for library purposes.

Enforcement and Redress

The library may conduct privacy audits to ensure that all library programs, services, employees and vendors are following this policy. Library users who have questions, complaints, or concerns about the way the library handles their privacy and confidentiality rights should send their comments in writing to the Library Director. The Director will respond in a timely manner and may conduct a privacy investigation or review of policy and procedures.

REQUEST FOR DISCLOSURE OF LIBRARY RECORDS

Definition of Library Records

For the purpose of this document, a library record is any document, record or other method of storing information retained, received, or generated by the library that identifies a person or

persons as having requested, used, or borrowed library materials, and all other records identifying the names of library users. Library records include records that identify users of electronic resources such as subscription databases, computer software, and web sites accessed through the Internet. Library records also include registrations for library-sponsored programs and events.

Requests from Library Users

Library staff shall comply with requests by a library user for any library record that identifies that user and library staff may require such request be in writing. Library staff may require photo or other identification to verify the identity of the person making the request, before releasing the information.

The parent or legal guardian of a minor may request library records that identify the minor. Library staff may require photo or other identification to verify the identity of the person making the request, and/or legal proof of guardianship, before releasing the information.

Library staff will not release any personally identifiable information contained in any library record to any other party without the express written consent of the person identified in the library record, or the express written consent of the parent or legal guardian of the minor identified in the library record.

Requests from Law Enforcement Officers

The Board of Trustees of the Scenic Regional Library authorizes the Library Director to receive all requests for library records from law enforcement officers. The Director will confer with the library's legal counsel before determining the proper response to such a request. The Scenic Regional Library shall not make any library record available to any agency of federal, state or local government unless a subpoena, warrant, court order or other investigatory document is issued by a court of competent jurisdiction that shows good cause and is in proper form.

In an instance of exigent threat, when the law enforcement officer has reasonable cause to believe that there is immediate danger of death, bodily harm, extensive property damage and/or public alarm and panic, the Board of Trustees authorizes the Library Director, upon advice of the library's legal counsel, to waive the requirement for a subpoena, warrant, court order or other investigatory document, and respond immediately to the officer's request, on the understanding that the appropriate documents subsequently will be provided by the officer.

No library employee except the Library Director is authorized to give out personally identifiable information from any patron record to any law enforcement officer. All such requests for information must be referred to the Library Director. It is lawful to refer an officer or agent to the Director even if the Director is not immediately available.

The passage of the USA Patriot Act has changed the ways in which the library responds to requests for information in some instances. Federal laws supersede state and local laws, and

there are differences in what is required based on the kind of order involved and the issuing authority.

Library employees shall follow these procedures:

- A local, state or federal officer or agent who **requests** information should be referred to the Library Director. It is lawful to refer the officer or agent to the Director even if the Director is not immediately available.

- Any local, state or federal officer or agent who presents a **subpoena** should be referred to the Library Director. It is lawful to refer the officer or agent to the Director even if the Director is not immediately available.

- If a local, state or federal agent presents a **search warrant**, library employees are required to stand back and allow the officer or agent to execute the warrant. Library employees should not interfere with their search or seizure. However, library employees should ask for a copy of the search warrant and contact the Library Director **immediately**.

- At the request of any local, state or federal agent, the library shall preserve computer terminal logs or records for 90 days pending the issuance of a court order or other process. Any local, state or federal agent may request, and the library shall grant, up to an additional 90 days for a total time period of maintenance of the records of 180 days.

- If a federal officer or agent (such as the **FBI**) arrives with a subpoena, warrant or court order issued pursuant to an investigation under the **USA Patriot Act**, library employees should contact the Library Director **immediately**. Also, be aware that the USA Patriot Act includes a **gag order** that prohibits library employees from sharing any information about the visit, the order or the information obtained under the order, with anyone other than their supervisor and the library's legal counsel.

Note: Should any employee be served with a subpoena or search warrant, notify the Library Director immediately. Call him/her office or call him/her at home. If the employee cannot reach the Director, they should call the Assistant Director at the office or at home. The Director or Assistant Director will call the library's attorney. An employee should not provide ANY information until they have talked to the Director or Assistant Director.

SOCIAL SECURITY NUMBER PRIVACY POLICY

SRL has adopted a Social Security Number Privacy Policy. The purpose of the Social Security Policy is to ensure, to the extent possible, the confidentiality of social security numbers, to prohibit the unlawful disclosure of social security numbers, to limit the persons who have access to the information and documents that contain social security numbers, and to set forth and practice proper procedures for the disposing of documents which contain social security numbers.

In the regular course of business, SRL collects and maintains documents which contain social security numbers, under conditions and circumstances allowed by law. In accordance with SRL policy, and as required by law, all or more than four (4) sequential digits of a social security number may not be placed on identification cards, badges, time cards, employee rosters, bulletin boards, permits, licenses, or any other materials or documents for public display. Documents, materials or computer screens that display all or more than four (4) sequential digits of a social security number may not be disclosed for public viewing and is limited only to authorized personnel who have a business reason for reviewing such information.

All documents containing social security numbers must be stored in a physically secure manner so that only authorized personnel have access to such information. Social security numbers may not be stored on computers or electronically unless they are secured from unauthorized access. Only management personnel who have legitimate business reasons to know may have access to records containing social security numbers. Social security numbers must be kept private and secure at all time. Documents may not be sent through the mail which contain all or more than four (4) sequential digits of a social security number, if the number can be seen through the envelope window or is otherwise visible from the outside of the envelope or package.

If documents containing social security numbers need to be disposed of, such disposal must be done in such a way to protect the confidentiality of the social security numbers. It is the policy of SRL that this is done by shredding.

Violations of the Social Security Privacy policy will result in discipline up to and including discharge. Employees are encouraged to immediately report any violations of this policy to the Associate Director of Business and Human Resources.