SANTA CRUZ PUBLIC LIBRARIES

Confidentiality of Library Records and Patron Data Privacy Policy

JPAB Policy # 303
Adopted: 6/6/2019
Five-year Review Schedule: 2024

The Santa Cruz City County Library System ("SCPL") complies with all sections of the State of California Public Records Act (Protection of Library Circulation and Registration Records, Government Code Title 1, Division 7, Chapter 3.5).

SCPL shall not disclose any registration, circulation, requests for reference information and Internet use records of library users to any person (except for a person acting within the scope of his or her duties within the administration of the library), or to any local, state, or federal agency except by order of the appropriate superior or federal court. SCPL may also disclose such information for authorized law enforcement investigations in emergency circumstances.

Santa Cruz Public Libraries adheres to the following best practices for securing patron data:

- Gather only the data SCPL considers necessary to perform the specific service.
- Keep the data only as long as SCPL deems it is needed to provide the service.
- Limit access to the data to those who use it in the performance of their duties.

DATA PRIVACY

The Santa Cruz Public Library System is committed to protecting the privacy of customers, staff, donors, and other contacts.

In order to protect library patron's data, SCPL requires customers to enter a unique Username and Password each time they want to access their account information.

Credit card information provided for fines and fees or services is used only for that intended purpose, and is transmitted via encryption, to a credit card processor. SCPL complies with all PCI-DSS standards.

NOTICE

SCPL strives to keep SCPL users informed of the policies governing the amount and retention of personally identifiable information, and about why that information is needed for the provision of library services.

Whenever SCPL policies change, notice of those changes shall be disseminated to SCPL users via the Library's website.

SCPL endeavors to avoid creating any unnecessary records, and to avoid retaining records not needed for providing or improving library services.

CHOICE & CONSENT

SCPL will only collect personal information for the administration of library services. Administrative services includes creation of hold records, fine billing and collection, marketing of library programs/services and creation of organizational statistics such as SCPL circulation, website visits and Wi-Fi use.

Patrons may choose to provide additional data such as preserving their circulation records to maintain personal reading lists or receive reading suggestions. If a patron voluntarily chooses to provide additional information, this information will be considered confidential.

SCPL will not sell, license or disclose personal information to any third party without patron consent, unless SCPL is compelled to do so by law.

SIGN-UP LISTS FOR COMPUTER WORKSTATIONS & ELECTRONIC COMPUTER RESERVATIONS

At some library branches, sign-up lists are maintained on paper to manage access to computer workstations. Those lists are shredded at the end of each day. In branches where a computerized reservation system is used, there is no electronic tracking of workstation use.

INFORMATION COLLECTED AND STORED AUTOMATICALLY

When a patron visits the SCPL website and browses through the web site, reads pages, or downloads information, certain information will be automatically gathered and stored electronically about the visit but not about the patron. This information does not identify individuals personally. SCPL automatically collects and stores only the following information about the website visit:

- The Internet domain and IP address from which access to our web site is gained;
- The type of browser and operating system used to access the Library's site;
- The date and time of access to the Library's site;
- The pages visited and for how long; and
- The address of the website from which the initial visit to www.santacruzpl.org was launched, if any.

SCPL uses this information to help it make its website more useful to visitors and to learn about the number of visitors to its site and the types of technology its visitors use.

LINKS TO OTHER SITES

SCPL's website contains links to purchase digital resources and other sites. The Santa Cruz Public Library System is not responsible for the privacy practices of these other sites, which may be different from the privacy practices described in this policy.

PATRON CIRCULATION RECORDS

SCPL maintains information provided by its customers from the registration form they complete when they register for a library card. SCPL does not use a paper process to collect and track customer circulation records. It is done electronically. When an item is checked out, that item is then tied to that customer's record in the library's electronic system. However, the moment that library material is returned to the library, the link between the customer and the material is broken – SCPL's system does not continue to retain information on such returned materials except as needed for payment of fines.

NETWORK SECURITY

For network security purposes and to ensure that the SCPL networks and Internet service remains available to all users, SCPL uses software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage to the SCPL network. If such monitoring reveals evidence of possible abuse or criminal activity, system personnel may provide the results of such monitoring to appropriate officials. SCPL does not attempt to identify individual users or their usage habits, however, SCPL recognizes that it may be compelled to identify such information, or disclose it, pursuant to an authorized law enforcement investigation or prosecution.

Unauthorized attempts to upload information or change information on this service are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1986 and 18 U.S.C. Sec. 1001 and 1030. Except for the above purposes, no other attempts are made to identify individual users.

SECURITY MEASURES

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. Managerial measures include internal organizational procedures that limit access to data and ensure that those individuals with access do not utilize the data for unauthorized purposes. 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 to un-authenticated users.

SCPL permits only authorized SCPL staff with assigned confidential passwords to access personal data stored in SCPL's computer system for the purpose of performing work within the administration of the library.

ENFORCEMENT & REDRESS

SCPL conducts regular privacy audits in order to ensure that all library programs and services are enforcing SCPL's privacy policy. Library users who have questions, concerns, or complaints about the library's handling of their private information should file written comments with the Director of the Library System. SCPL will attempt to respond in a timely manner.

PRIVACY & CONFIDENTIALITY OF LIBRARY RECORDS

The Santa Cruz Public Library System respects the right of privacy of all its customers regarding the use of this Library System. Library records are protected under California Government Code, Title 1, Division 7, Sections 6250-6270, Chapter 3.5.

REVISIONS

SCPL reserves the right to change or modify this privacy statement at any time. If SCPL revises this privacy statement, changes will be posted on the Library's homepage.

Excerpt from State of California PUBLIC RECORDS ACT

(Protection of Library Circulation and Registration Records)
(Government Code title 1, Division 7, Chapter 3.5)

Cal. Gov. Code Sec. 6254. Records exempt from disclosure requirements.

Except as provided in Sections 6254.7 and 6254.13, this chapter does not require the disclosure of any of the following records:

(j) Library circulation records kept for the purpose of identifying the borrower of items available in libraries, and library and museum materials made or acquired and presented solely for reference or exhibition purposes. The exemption in this subdivision shall not apply to records of fines imposed on such borrowers.

***

Cal. Gov. Code Sec. 6254.5 Disclosure of otherwise exempt records; Exceptions.

Notwithstanding any other law, if a state or local agency discloses a public record that is otherwise exempt from this chapter, to a member of the public, this disclosure shall constitute a waiver of the exemptions specified in Sections 6254, 6254.7, or other similar provisions of law. For purposes of this section, "agency" includes a member, agent, officer, or employee of the agency acting within the scope of his or her membership, agency, office, or employment.

This section, however, shall not apply to disclosures:

(a) Made pursuant to the Information Practices Act (Chapter 1 (commencing with Section 1798) of Title 1.8 Part 4 of Division 3 of the Civil Code) or discovery proceedings.

(b) Made through other legal proceedings or as otherwise required by law.

(c) Within the scope of disclosure of a statute that limits disclosure of specified writings to certain purposes.

(d) Not required by law, and prohibited by formal action of an elected legislative body of the local agency that retains the writings.

(e) Made to any governmental agency that agrees to treat the disclosed material as confidential. Only persons authorized in writing by the person in charge of the agency shall be permitted to obtain the information. Any information obtained by the agency shall only be used for purposes that are consistent with existing law.

Cal. Gov. Code Sec. 6255. Withholding records from inspection; Justification; Public interest.

(a) The agency shall justify withholding any record by demonstrating that the record in question is exempt under express provisions of this chapter or that on the facts of the particular case the public interest served by not disclosing the record public clearly outweighs the public interest served by disclosure of the record.

***

Cal. Gov. Code Sec. 6267. Confidentiality of patron use records of any library supported by public funds; Exceptions; "Patron use records".

All patron use records of any library which is in whole or in part supported by public funds shall remain confidential and shall not be disclosed by a public agency, or private actor that maintains or stores patron use records on behalf of a public agency, to any person, local agency, or state agency except as follows:

(a) By a person acting within the scope of his or her duties within the administration of the library.

(b) By a person authorized, in writing, by the individual to whom the records pertain, to inspect the records.

(c) By order of the appropriate superior court.

As used in this section, the term "patron use records" includes the following:

(1) Any written or electronic record, that is used to identify the patron, including, but not limited to, a patron's name, address, telephone number, or e-mail address, that a library patron provides in order to become eligible to borrow or use books and other materials.

(2) Any written record or electronic transaction that identifies a patron's borrowing information or use of library information resources, including, but not limited to, database search records, borrowing records, class records, and any other personally identifiable uses of library resources information requests, or inquiries.

This section shall not apply to statistical reports of patron use nor to records of fines collected by the library.

Excerpt from COMPUTER FRAUD and ABUSE ACT of 1986

18 USCS §1030. Fraud and related activity in connection with computers

(a) Whoever—

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

(5)(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States;

(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any—

(A) threat to cause damage to a protected computer;

(B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or

(C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion;

shall be punished as provided in subsection (c) of this section.