LIBRARY FREEDOM PROJECT

LIBRARY PRIVACY POLICY TEMPLATE

General Privacy Policy/Statement

Your privacy is important to us and we do everything we can to protect and respect your personal information and keep your library records confidential. The library strives to collect the least amount of personally identifiable information we can and avoids creating unnecessary records. The library does not share your personally identifiable information with third parties unless served with a valid subpoena, national security letter, or warrant to do so.

The Library follows [link to Your State and/or Local Law] which requires all public libraries in [Your State] to guarantee the privacy of user records.

What information do we collect?

The library collects both personally identifiable information (PII) and anonymous information in order to provide library service to users.

Personally identifiable information is any information that could potentially identify a specific individual. The library strives to collect the least amount of personally identifiable information possible in order to provide services. We avoid creating unnecessary records. The personally identifiable information collected by the library could include:

- Name
- Address
- Telephone Number
- Email address

- Date of Birth
- Library barcode number
- Items currently checked-out, requested, canceled holds, and interlibrary loans
- Overdue items (until returned)
- Fine history
- Sign-up information for library classes and events

Anonymous information is information that does not specifically identify an individual. The anonymous information collected by the library could include:

- URL (uniform resource locator) of the web site you visited previous to the library's website
- Domain names and/or IP addresses (numbers automatically assigned to your computer whenever you are connected to the internet)
- The browser version you are using to access the web site
- Hardware and software type and language
- Cookie data
- Date and time of requests
- Demographic data
- Interaction data
- Page Views, click data, and navigation flow

Who has access to it?

All library user records are confidential. Library records may only be disclosed to:

- Library staff performing job duties
- Cardholders upon proof of identity
- Anyone with the library card number
    - Only share your card number with people you trust and report lost or stolen cards immediately
- Law enforcement with a valid subpoena, national security letter, or warrant

Library materials and borrowing history

The library does not keep a record of your borrowing history beyond operational requirements. Once you return an item, it is removed from your account. Items with lost or damaged fees will remain on your account until paid.

Radio Frequency Identification (RFID) technology is used to check out library materials, keep a record of the library collection, and secure the collection from theft. RFID tags attached to items only contain the barcode number of the item. No personal library user or transaction information is on the RFID tag.

Public computers and wireless network

The library does not keep a record of your activities on any public computer or on our wireless network. Any record of browsing history and activities on our public computers or wireless network are removed when you log out or disconnect. Information about your public computer reservation (library card number, computer number, reservation time, and session duration) is purged at the end of each day.

Surveillance cameras

Several of our libraries have security cameras outside and/or inside. Video footage is kept for [#] days. Video is only available to view by [supervisory staff]. A valid subpoena, national security letter, or warrant is required to view footage from indoor cameras.

Security Officers have body-worn cameras. They can record user contacts, interviews, and other events when recording could provide value as evidence. Before recording, an officer issues a verbal announcement to the user. Video footage is kept for [#] days. This video is only available to view by [supervisory staff].

Library website

HTTPS

The library's website is encrypted with HTTPS. All communications between your browser and the library website are private. Your account and catalog searching is also encrypted [OR (if not secure) Your catalog searches and browsing activities are not.]

Cookies

Some library applications use what are called "cookies." A cookie is a small file created by a website and saved by your browser each time a site is visited. Cookies are stored on your computer and can transmit personal information. Cookies are used to remember information about preferences and customization on the pages you visit. You can refuse to accept cookies, disable cookies, and remove cookies from your hard drive by following the instructions provided by your browser. Some third-party services may not work if cookies are disabled.

Data & network security

The library is committed to data security and keeping your personally identifiable information that is collected by our website safe. The library monitors network activity to identify unauthorized attempts to upload or change information or otherwise cause damage. The library

operates secure data networks protected by industry standard firewalls and password protection systems. Only authorized individuals have access to the information provided by our users.

Children's privacy

The safety and privacy of children is very important to the library. As with all other patrons, personal information collected from children by the library is not shared with any non-contracted agency or vendor. We encourage parents to take an active role in their children's internet use and teach them about the importance of not revealing personal information online.

Non-library websites

Non-library websites may be linked through the library's website and may not follow the same privacy policies as the library. Non-library websites include some of the links from our Web Resources, Adult Literacy Resources, Jobs & Money, and others [list of places with concentrations of web links] dispersed throughout the library website. Visitors to such sites are advised to check the privacy statements of such sites and to be cautious about providing personally identifiable information without a clear understanding of how the information will be used.

Third-party vendors

Note: Some online services offered by the library are serviced by third-party vendors. These vendors have their own privacy policies and terms of service and they are not beholden to the library's privacy policies or terms or service.

The library works with third-party vendors to provide online learning, digital collections, streaming media content, analytics, and more. These third-party vendors include providers like Overdrive/Libby, Kanopy, Hoopla, Facebook, Instagram, Gale databases, and more [list some of your popular vendors]. When you leave the library website, your interaction with these systems will be governed by their individual privacy policies. Some of these vendors may collect and share information you provide to them or require you to create a personal account in order to use their services. Check the vendor's privacy statement and terms of service to learn more about how your data is tracked, stored, and used by them. We have provided links to individual privacy policies and terms of statements for a majority of our third-party vendors for your review. [If some vendors do not have a privacy policy: Some vendors do not have a public facing privacy policy or terms or services. We have noted vendors with no public policy; please exercise caution when visiting these vendors or providing personal information to them.] Inquire with the vendors directly if you have any specific questions about their data collection and management policies.

[Include link to page with links to third party vendor policies] LAPL Example

LIBRARY FREEDOM PROJECT

LIBRARY VENDOR PRIVACY ASSESSMENT

The following list of questions can be asked of vendors to help your library assess their privacy policies and procedures:

- What data do you collect? Why? Do you collect personal identifying information? Is data anonymized or de-identified?
- Do you have a publicly listed and easy to locate privacy policy?
- Is data sold to/shared with third parties?
- What is your policy on sharing data with law enforcement or government agencies?
- Is data protected at all phases and stored securely?
- How long do you retain user data?
- Do users opt-in to data collection and use by default? What are users' opt-out options?
- Do you adhere to all of *the library's* local, state, and national laws on privacy and make changes when new laws are adapted?
- Where is the data stored? Is data stored in a country other than the library's?
- Are users allowed to delete their data?
- Are users allowed to delete their account? Will their data also be deleted?
- Have there been any data breaches? How quickly did you respond? What are your accountability practices?
- What web standards do you apply? SSL, HTTPS, TLS (which version), Strong token, weak hash, plaintext?
- How do users log in? Library card/PIN preferred. Do users need to create a separate account to create?

INSTITUTE of Museum and Library SERVICES

We created this resource thanks to the support
of the Institute of Museum and Library Services.