Safe Data
Safe Families

Privacy Policy Framework

safedata.umd.edu | 2021

INSTITUTE of Museum and Library SERVICES

UNIVERSITY OF MARYLAND 18 56

COLLEGE OF INFORMATION STUDIES

Table of Contents

How to Use the Safe Data | Safe Families Privacy Policy Framework

The Safe Data | Safe Families Privacy Policy Framework is meant as a companion piece to the American Library Association (ALA) Privacy Toolkit (http://www.ala.org/advocacy/privacy/toolkit), which provides useful information for creating or revising a privacy policy. ALA's Toolkit focuses on how libraries--as an institution--can protect patron's privacy, including how to protect the information that libraries receive from patrons during traditional library transactions. Our privacy policy framework supplements ALA's Toolkit by focusing on library staff interactions with patrons and covers many of the day-to-day privacy risks patrons face. This framework also addresses some of the tensions that library staff face between helping patrons and liability issues related to patrons' personal information.

Our research with library staff from around the United States has highlighted that each library and library system is unique and comes with its own unique views and challenges related to their location, their population's needs, and more. This framework is meant to provide you with some flexibility in thinking about staff-patron interactions and to reduce uncertainty about how to respond to patron requests involving personal information. We recognize there are exceptions to every policy and that we may not cover the specific situations you experience at your branch, but we try to provide examples from existing policies at public libraries whenever possible to show how other branches have implemented various types of policy.

First, you will find an introductory section on *Responding to Patron Requests: What Staff Can and Cannot Do*. Next, you will find the privacy policy framework organized into six sections: *General Patron Privacy Concerns*, *Protecting Financial Information Online*, *Privacy When Completing Online Forms*, *Privacy When Accessing Library Contracted Third-Party Sites*, *Special Considerations for Minors*, and *Privacy at Public Computers*. Finally, you will find a section on

Tips to Communicate Your Library Privacy Policy and one on *Additional Resources for Crafting your Library Policy*.

Responding to Patron Requests: What Staff Can and Cannot Do

Your patrons will likely vary significantly in their skill level when using technology. Helping patrons who may have lower digital literacy skills can introduce several privacy challenges, especially when they need assistance with a website or app that is asking for sensitive personal information. Patrons may ask for help creating an account, applying for a job, or filing their taxes.

The best policy in these cases is to make decisions that align with your library's policies and guidelines while protecting the patron's privacy as much as possible and remaining within your comfort zone. These situations can provide a useful backdrop for having conversations with patrons about digital privacy and security. That said, there will be times when patrons will request task-oriented assistance but won't want to take the time to learn about *why* data privacy matters. It will be up to staff to determine whether there is enough time to help the patron develop these skills or simply provide help with their request.

The following examples include statements shared publicly on some libraries' websites on how they have addressed how staff should handle patron requests involving technology use and data entry, and how much time staff should devote to a single patron.

Examples

> *"Staff will devote a reasonable amount of time assisting individual library patrons with the Internet where needed. They cannot devote large amounts of time to each customer because staff members are handling information requests from many individuals. Regular programs, demonstrations, and hands-on sessions on the use of the Internet are provided by the library staff*

and are available to all patrons. Attendance at such programs may require sign-up in advance, depending on demand." ***--Pasco County Libraries (Florida)***

"Staff members are trained to assist customers in using the Library catalog and Web site as well as databases and other Web services selected and purchased by the Library. In some cases, vendor assistance is needed to resolve problems with or to answer specialized questions about these services." ***--Monterey Public Library (California)***

"Security for personal devices rests solely with the owner. Library staff members may provide guidance for accessing library materials and services, but they do not provide technical support." *--**Ames Public Library (Iowa)***

"Library staff must take appropriate actions to resolve problems which arise during use of the Library's computer and Internet services and to enforce Library policies and rules. To this end, Library staff members may need to observe computer use, question users, and restrict conduct by users which violates this policy." ***--Monterey Public Library (California)***

"Library staff members are available to assist patrons of all ages with information literacy: to access information efficiently and effectively, evaluate information critically and competently and use information accurately and creatively." ***--San Antonio Public Library (Texas)***

General Patron Privacy Concerns

Patrons using library computers or personal devices in the library may encounter many privacy risks while going about their daily business. These risks include account and password creation, submitting online forms, and using social media.

Key Topics

Password and login help

In order to protect patrons' privacy, policies limiting how much staff can do with patron passwords are necessary. In our work, library staff said they spend a significant amount of time helping patrons with their passwords--creating new ones, recovering forgotten ones, and explaining to patrons why they can't write down or remember a password for the patron.

Mobile devices (patron owned)

Most patrons now own a smartphone, tablet, and/or e-reader, and they may be able to access various library services through their own devices. That said, troubleshooting these problems for patrons can be difficult; there many different operating systems and models of device and library staff are unlikely to be familiar with all of them. Staff may also not want to personally handle these devices because of liability issues. Patrons may get frustrated with staff trying to walk them through an issue, or they may ask staff to fix the problem for them. In our research, many library staff indicated that it would be helpful if there were clear guidelines on how much help they can and should give patrons.

Mobile devices (library owned)

Some libraries loan mobile phones, tablets, Wifi hotspots, or laptops to patrons. Patrons may not know what happens when a checked-out device gets checked back in with the library. Library staff should be transparent about what process is in place, if any, to delete patron data

before the device is checked out by another patron, and provide patrons with best practices to prevent personal information from being stored on these devices.

Library Wifi

For many people, public libraries are one of the few places that provide free access to WiFi. However, with all public WiFi, there are risks to users' privacy. Steps should be taken to both reduce these risks and to inform patrons of any risks associated with public WiFi.

Social Media

Social media is now used by most American adults, and people may share a lot of private information via Facebook, Instagram, Twitter, and other social media platforms. There are ways to reduce privacy risks associated with social media, and it is important to both explain these risks to patrons and also show them how to change their privacy settings.

Recommended Actions

Decide on a policy of how much support staff can provide when helping patrons with password management. For example, can staff type in the password? Or is this something that needs to be done by the patron? In our research, several library staff recommended having patrons enter passwords in most situations because that empowered them and reinforced to them that it was something they were capable of doing, but there may be times when exceptions need to be made. This is something that should be discussed and decided upon so that staff have clear guidelines for what to do in these patron interactions.

Staff members should limit their handling of patrons' devices. Our research has shown that many library systems prohibit staff from touching devices; in practice, however, it is sometimes necessary for staff to handle patrons' smartphones and other devices, such as when a patron has mobility limitations. When handling a patron's device, recommended guidelines include keeping within sight of the patron when handling their device, making sure patrons are in

charge of agreeing to terms or accepting cookies, or making sure that patrons are always the ones holding their device.

Provide patrons with clear guidelines on how to create strong and memorable passwords, and how to reset passwords. Remind patrons that passwords should not be shared with anyone, even library staff. See the Safe Data | Safe Families Teaching Moments resource on *Creating Strong Passwords*.

Check with your library's IT person/department regarding the security settings of the wireless network. Communicate any risks of using the WiFi with patrons. Consider adding a warning to a landing page.

Provide information to patrons on how to adjust their privacy settings on social media. See the Safe Data | Safe Families Teaching Moments resources on *Changing Privacy Settings on Facebook* and *Who Can See My Social Media Posts?*.

Library staff should strive for transparency in communicating library practices concerning patron privacy and confidentiality parameters.

Develop a mobile device borrowing policy. This policy can communicate the following to patrons:

- Who can borrow a mobile device?
- How long a device can be checked out for?
- Where the device can be used?
- What accessories are provided when a device is borrowed (ex. chargers)?
- Any associated fines or fees for device returned late or damaged
- What to do if the patron notices damage?
- What patrons can and cannot do with the device?
- What happens to the patron's personal data that are stored in the device?

As devices are constantly changing, policies will have to adapt. Therefore, the policy should include a disclaimer about the library's right to change or modify the policy.

Examples of Library Policy:

> *"Library staff will help you use the computers to find the information you need. Library staff and volunteers also will help you learn to use search tools on the Internet computers, although they cannot provide extensive one-on-one instruction."* ***--Multnomah County Public Library (Oregon)***

> *"All devices are the responsibility of the owner. Library staff is not allowed to configure patron's equipment, nor can they provide more than general assistance in getting connected to the internet."* ***--Nocona Public Library (Texas)***

> *"The wireless connection provides less security than wired networks; users should exercise caution when transmitting credit card numbers or other sensitive information. Users are urged to protect their computers with firewall software and data encryption."* ***--Acton Memorial Library (Massachusetts)***

> *"The Library's WiFi does not provide a secure connection. Patrons use the Library's wireless Internet access at their own risk. The Library encourages patrons to use virus protection, a personal firewall, and other measures to protect personal information from disclosure. Patrons using their portable computing devices are solely responsible for protecting their personal information and assume all risks of an invasion of privacy or disclosure of personal information that may occur when using the Library's WiFi."* ***--Boulder Junction Public Library (Wisconsin)***

> *"Users should also be aware that another wireless user may be able to view or change files on any wireless user's computer. The Library recommends that users install and use virus protection software, firewall software, and security patches or upgrades to identify and eliminate viruses in any data, files, or programs they obtain from external computers or networks, and to protect their computers from intrusion."* ***--Monterey Public Library (California)***

> *"SFPL champions the protection of personal privacy. SFPL will keep confidential all such information that it purposefully or inadvertently collects or maintains to the fullest extent permitted by federal state and local law, including the*

California Public Records Act, the San Francisco Sunshine Ordinance, and the USA PATRIOT Act.

- *The Internet is not a secure medium. Email is not necessarily secure against interception.*
- *The Library does not monitor an individual's use of the Internet. Computer search stations are programmed to delete the history of a user's Internet session once the session is ended. The Computer Booking history is deleted every day.*
- *Internet computers are provided with privacy screens for your privacy. In accessing various Internet sites, please be conscious of others in your vicinity, particularly children.*
- *SFPL does not provide information about patrons' library records, use of other SFPL materials, or use of the Internet to law enforcement officials without an appropriate court order. However, law enforcement officers may take action on their own if they observe illegal activity in plain view. Internet users are reminded that illegal use of the Internet is prohibited by State and Federal laws, and by SFPL policy."*

--San Francisco Public Library (California)

"The Library uses an online computer reservation program that allows the public to reserve a computer in order to access the Library's catalog, the Internet and other resources. The Library's public computer search stations are programmed to delete the history of a library user's Internet session and all searches once an individual session is completed. Booking history is deleted every day." ***--San Francisco Public Library (California)***

"Enhancements to the Library's online catalog system that offer greater functionality and customized features that may impact user confidentiality will be activated by the Library only if such enhancements are optional to the user. Use of enhancements is governed by privacy statements and terms and conditions of the vendor." ***--San Francisco Public Library (California)***

"The Library reserves the right to modify the Mobile Device policy and Mobile Device Borrower Agreement at any time. Blocking software is not available on mobile devices and the library cannot be held responsible for any content viewed. By checking out a mobile device, the patron agrees they will not engage in illegal activities, they are solely responsible for the mobile device, and they are eighteen years or older. The library is not responsible for loss or damage to

patron's data for any reason while the patron uses a library mobile device." **--Eastern Monroe Public Library (Pennsylvania)**

The Internet offers access to a wealth of material that is personally, professionally and culturally enriching to individuals of all ages. However, it also enables access to some material that may be offensive, disturbing, illegal, inaccurate or incomplete. Users are encouraged to evaluate the validity and appropriateness of information accessed via the Internet. **--Multnomah County Library**

Protecting Financial Information Online

Shopping and banking online can put your patrons' financial information at risk. Sharing sensitive information like credit card numbers, financial information, and personal addresses on public computers, when using unencrypted websites, or while using public WiFi are especially risky.

Key Topics

Protecting patrons' financial information

With libraries being one of the few options for free public WiFi, some patrons will need to enter their credit card or bank information on library computers. There are risks that come with entering financial information this way, and it is important that library staff communicate these risks to patrons and help their patrons with these transactions while maintaining patron privacy.

Identifying and reporting scams

Many libraries work with vulnerable populations that are at increased risk of being targeted by scams and identity theft. It is important for library staff to be well versed in common scams so they can identify them and communicate these risks with patrons.

Recommended Actions

Advise patrons to look for the secure symbol in the address bar (https) before entering private information. For specific browsers, find more information here:

- Firefox: https://support.mozilla.org/en-US/kb/how-do-i-tell-if-my-connection-is-secure
- Chrome: https://support.google.com/chrome/answer/95617?hl=en

- Safari: https://support.apple.com/guide/safari/avoid-fraud-by-using-encrypted-websites-sfri40697/mac

Set a policy on how much help staff can give patrons when it comes to entering financial information, such as credit card and bank information. When determining this policy point, discuss boundaries and limitations. Are there exceptions to the policy? What variables would necessitate leniency?

Ensure library staff are made aware of current scams and how to spot them. These could be raised in staff meetings or posted to an online training space. The Federal Trade Commission offers resources on how to spot a scam, which can be found here: https://www.consumer.ftc.gov/articles/how-avoid-scam. See the Safe Data | Safe Families Teaching Moments resources for *How to Spot a Phishing Scam* and *Shopping Safely Online*. Additionally, consider creating a page on your website to educate patrons about scams, like the one at the Hawaii State Public Library System.

Examples of Library Policy

> *"Privacy while using the Internet in the library cannot be guaranteed. There exists a possibility of inadvertent viewing by others. Customers handling financial transactions or other activities that require confidentiality do so at their own risk. The Internet is not a private environment and security of electronic communication cannot be guaranteed."* ***--Ames Public Library (Iowa)***
>
> *"The Library's wireless Internet service is not encrypted. Users should be aware that any information sent or received could potentially be intercepted by another wireless user. Web-based security controls such as Secure Sockets Layer (SSL) are not sufficient to protect against certain types of attacks; therefore, users should avoid entering sensitive information such as credit card numbers, passwords or any other personally identifying information on any wireless network."* ***--Monterey Public Library (California)***
>
> *"Avoid entering credit card numbers, passwords or other confidential information until you can verify that the Web site you are interacting with*

provides its own security mechanism such as SSL (Secure Sockets Layer) encoding. An SSL-protected Web page usually displays a small lock icon along the lower edge of your browser window. We strongly urge you not to use library computers for transfer of any sensitive information." ***--South Thomaston Public Library (Maine)***

Privacy When Completing Online Forms

Many official forms like taxes, healthcare, and unemployment are now completed online. Patrons should be extra aware of where they are entering their private information and ensuring that they are on an official and secure site.

Key Topics

Liability concerns, especially with taxes, medical / insurance forms

The library is often used by patrons to access official government paperwork like taxes and insurance. However, this access does not come with built-in help and often requires users to enter personal information like their social security number. In our research with library staff, several raised potential problems with patrons coming to the library to submit these forms.

How to navigate to the correct (free) site

Some government forms like tax filing and the FAFSA are free to file, but unofficial sites often charge for these documents. Likewise, some scams attempt to direct people to fake government websites to prompt them to enter personal information.

Job hunting

Looking for jobs often requires job hunters to submit sensitive information, like social security numbers and other personally identifiable information to websites and third-party sites like Indeed. This can make job hunters vulnerable if their information is not protected on these third-party sites (see also section on *Privacy When Accessing Library Contracted Third-Party Sites*).

Recommended Actions

Consider partnering with external institutions to offer programming or workshops to patrons on how to protect their privacy when completing online forms. For example, the AARP Foundation has offered a free Tax-Aide Service for adults ages 50 and older. When working with external partners, take time to vet the presentation and ensure the information being shared with patrons is consistent with library privacy policy and recommendations.

Create a document list or bookmark the most visited sites for patrons (unemployment, taxes, FAFSA, etc.) on the library's public computers to ensure that patrons are able to access free government resources.

Set limits on how much staff can help their patrons when completing online forms. Staff should not directly help with completing tax documents, but can help troubleshoot technical problems.

Inform patrons about available resources on protecting their privacy online. You can point them to resources such as the Identity Theft Resource Center, or the Federal Trade Commission's websites on identity theft and online security tips and resources.

Examples of Library Policy

> *Staff members assist customers with all computer, Internet, and other technology questions… providing answers, print or Web resources, and/or referrals for further information, assistance, and training. Staff cannot provide extended individual training or technical support.* ***--Monterey Public Library (California)***
>
> *"In choosing sources to link to from its home pages, the Library follows its materials selection guidelines. Beyond this, the Library is not responsible for the content of the Internet, changes in content of the sources to which the Library home pages link, or for the content of sources accessed through secondary links."* ***--New York Public Library***
>
> *"In an effort to assist its users, the Library has created websites for the general population, for teens, and for children to help guide them to sources that are accurate, complete, and current and that provide them with a wealth of information on the local, national, and global level. In addition, the Library*

provides training for members of the public to assist them in using the Internet in a safe, effective, and efficient manner." ***--New York Public Library***

Privacy When Accessing Library Contracted Third-Party Sites

Third-party sites and applications used in the library for ebooks, e-learning, or other library services have their own privacy policies that may not align with the library's privacy goals or beliefs.

Key Topics

Privacy on third-party sites

Though libraries may partner with third parties like *Overdrive* and *LinkedIn Learning*, this does not mean that these third parties have the same privacy standards that libraries have. Therefore, it is important to ensure that patrons are aware that their privacy is not regarded the same between platforms.

Recommended Actions

Explicitly state when a patron leaves the library website and goes to a third-party website. Communicate with patrons about the possible privacy risks when navigating to third-party sites.

It is impractical for all staff to understand all of the privacy policies of the third parties associated with the library. However, if a library is thinking about adopting a third-party program/tool, they should engage in a vetting process before adding it. For guidance on how to do this, consult ALA's guidance and the Library Freedom Vendor Privacy Audit. There are privacy policy ratings of popular vendors available, such as the Library Freedom Vendor Privacy Scorecard.

Examples of Library Policy

"When connecting to licensed databases and content providers outside the library, CCPL only releases information that authenticates users. Nevertheless, when accessing remote or third party vendor sites, there are limits to the privacy protection the library can provide." ***--Cecil County Public Library (Maryland)***

"In choosing sources to link to from its home pages, the Library follows its materials selection guidelines. Beyond this, the Library is not responsible for the content of the Internet, changes in content of the sources to which the Library home pages link, or for the content of sources accessed through secondary links. " ***--New York Public Library***

"Boise Public Library works with 3rd party vendors to deliver online services, digital collections, streaming media content, and more. We strive to ensure the library's contracts, licenses, and offsite computer service arrangements reflect our policies and legal obligations when it comes to customer privacy and confidentiality. For example, the library expects vendors to follow all privacy-related items in the vendor contract and licensing agreements; conform to library privacy policies; provide a product that complies with the Children's Online Privacy Protection Act; and refrain from collecting or sharing information about customers other than what's needed for delivery of the library services in question. Because third-party vendors operate with their own terms, there are limits to the privacy protection we can offer when you use their services." ***-- Boise Public Library (Idaho)***

"San José Public Library licenses services and content from third-party vendors who have their own privacy policies and confidentiality practices. When you leave the library website, your interaction with these systems will be governed by their individual privacy policies." [followed by a list of vendors with links to their privacy policies] ***--San Jose Public Library (California)***

"Our Confidentiality and Privacy Policy may not extend to the services and content we offer through third party vendors, which range from digital collections to reference resources to some of our background systems. If you use library services provided through these companies, your interaction is subjected to the privacy policies and confidentiality practices of that specific vendor. Check their privacy statements to learn more about what data they store and how they use it." [followed by a list of vendors with links to their privacy policies] ***--Iowa City Public Library (Iowa)***

"Please exercise discretion when browsing the Internet. You should be aware that when you are on our website, you could be directed to other sites that are

beyond our control. These other sites ('External Sites') may send their own 'cookies' to users, collect data, solicit personal information, or contain information that you may find inappropriate or offensive." ***--Wayne Public Library (New Jersey)***

"The Library's web site contains links to other sites. BCLD is not responsible for the privacy practices of other sites, which may be different from the privacy practices described in this policy. We encourage you to become familiar with privacy practices of other sites you visit, including linked sites." ***--Berthoud Community Library District (Colorado)***

Special Considerations for Minors

Children and teens spend a great deal of time online and may not know or understand how their actions can put personal information at risk. These risks are most likely to occur when minors use social media or online chat (e.g., when playing games).

Key Topics

Helping minors protect their identity

To help protect minors online, it is important to provide guidelines designed to warn them of the dangers of talking to strangers on the internet and sharing personal information through online channels. The library may employ various filters to prevent children from accessing certain types of content, but these filters are limited in their scope.

Social Media and Privacy

Minors on social media are especially at risk to being targeted by predators. Library staff can help minors protect themselves on social media by assisting them with the privacy settings on their accounts.

Recommended Actions

Consult the Children's Internet Protection Act (CIPA) for guidelines on protecting minors online.

Consult the Children's Online Privacy Protection Act (COPPA) website for Frequently Asked Questions on complying with COPPA.

Make sure language in policy can be understood by minors (no technical language or jargon).

Encourage parents and minors to learn more about online safety by sharing links to existing resources. Some examples include:

- FTC's Protecting Kids Online program (https://www.consumer.ftc.gov/topics/protecting-kids-online) is a federal government website with resources on how to protect kids online.
- Google's Be Internet Awesome (https://beinternetawesome.withgoogle.com/en_us) is a program that provides educational resources for children to learn more about technology and online safety.
- ConnectSafely (http://www.connectsafely.org/) is a non-profit organization that provides useful safety tips and advice for parents and teens.
- Safe Data | Safe Families Teaching Moments resources (*Advice for Parents: Talk to Your Teen About Social Media, Advice for Teens: Manage Your Digital Footprint, Advice for Teens: Managing Social Media, and Keeping Kids Safe: Avoiding Bullying Online*)

Examples of Library Policy

*"**New York Public Library**'s guidelines for minors:*

- *Never give out identifying information such as home address, school name, or telephone number.*
- *Let parents or guardians decide whether personal information such as age, marital status, or financial information should be revealed.*
- *Never arrange a face-to-face meeting with someone via the computer without parents' or guardians' approval.*
- *Never respond to messages that are suggestive, obscene, threatening, or make one uncomfortable.*
- *Have parents or guardians report an incident to the National Center for Missing and Exploited Children at 1-800-843-5678 if one becomes aware of the transmission of child pornography.*
- *Remember that people online may not be who they say they are.*
- *Remember that everything one reads may not be true."*

*"All computers in the designated children's area are only for use by children age 12 and younger and for parents or caregivers assisting children." **--DC Public Library***

"The San Antonio Public Library's goal is for children to have safe online experiences and prevent their exposure to harmful or inappropriate material. Library Board Policy on Public Use of the Internet San Antonio Public Library. Towards this goal, the San Antonio Public Library has taken the following initiatives:

- *Filtering Internet access for images and videos containing adult content that would generally be considered obscene or pornographic in nature.*
- *Encouraging parents to monitor and supervise their own children's use of the Library's computers and networks.*
- *Providing specially designed web pages for children and teens.*
- *Providing child-friendly search engines on the children's page.*
- *Providing links to sites that help children learn Internet safety.*
- *Providing staff who are trained to help children and parents find appropriate sites.*
- *Enforcement of this policy." --* ***San Antonio Public Library***

*"The Library provides Web pages, links, databases, and other online resources to guide young users to useful, interesting, educational, appropriate, and fun sites selected by Library staff. Whenever possible, Library staff members assist young customers in locating and choosing appropriate and useful Internet resources, and guide young customers away from inappropriate sites. Library policy gives parents or guardians the right and responsibility to restrict their children's and only their own children's use of Library resources, including computers and the Internet. The Library respects the right of parents to determine what it is appropriate for their children to read, hear, and view, but the Library cannot enforce these rules, which may be different for each family in our community. Parents are encouraged to supervise and to participate actively in their children's computer and Internet use. The Library does not act in loco parentis: It does not have the same role in supervising children that schools have, and it cannot substitute its judgment for that of parents or enforce parents' decisions about their children's Internet use." --***Monterey Public Library (California)***

*"The Library strongly encourages parents or legal guardians to supervise their children's Internet use and to provide them with guidelines about acceptable use. It is the responsibility of parents and/or guardians to instruct their children not to give private information about themselves or others, when using web sites or e-mail." --***Dormont Public Library (Pennsylvania)**

"Parents, guardians, and caregivers are expected to instruct minors to safely share personal information (name, address, password, telephone number, school, credit card number, etc.) on the Internet. This includes but is not limited to email, instant messaging, online purchasing, social media sites, and commercial sites. Before giving out any personal information via email, minors need to be confident that they are dealing with someone who is known and trusted by them and their parents or guardians." ***--Madison Public Library (Wisconsin)***

Privacy at Public Computers

On public computers, patrons face privacy risks online and offline. Remind patrons to keep their private information close, lock their computer if they need to step away, and completely sign out when they are done. While there are risks to using public computers and public wifi, sometimes this may be the only option available to patrons.

Key Topics

Install session management systems

Adding session management systems will delete all personal information saved during a patron's session and is a way to keep patrons' information secure, even if individuals are not able to do so themselves.

Encouraging patrons not to share their private information with library staff

Library staff are often seen as people who can be trusted; this often means that patrons are willing to give staff much of their personal information if it means they can get the help they need. This can lead to uncomfortable situations for the library staff (such as patrons sharing their private information loudly in the library) and is a risky privacy behavior in a public space.

Computer Setting in Library

How public computers are organized in the physical environment of the library can have a big impact on how private computers are for patrons. This extends to other digital equipment in libraries like printers and scanners.

Using the Public Copier, Printer, and Scanner

Using the copier or printer at the library is a convenient resource for the community, but it is important that patrons are aware that these resources are public and that it is important that

they promptly pick up their printed materials and not leave their materials (like their driver's license or social security card) at the copier or scanner. In addition, libraries should ensure that patron's data is not stored on these resources.

Recommended Actions

If your library does not currently have a session management system, consider getting one. If this isn't an option, consider setting up guidelines and a process to routinely delete personal information manually on public computers.

Set guidelines and language to address how staff can limit the amount of patron data they are told.

Ensure that patron's data is not kept on library's digital devices like printers and scanners.

Ensure that the physical space of computers and digital devices are configured for maximum privacy - situate screens so they are not easily visible to major foot traffic, ensure that video and photos are not used in this area and that security cameras are not capturing the screen of a public computer.

Encourage the use of privacy screens, and encourage patrons to follow acceptable use policies.

Examples of Library Policy

> *"...the Library is a public place, and the Library cannot provide private computer workstations or seating areas. At the same time, passersby should respect the privacy of computer users, and computer users should not attempt to show displayed material to passersby."* ***--Monterey Public Library (California)***
>
> *Users of Library workstations are asked to use resources appropriately and respect the privacy of others using nearby workstations...The Library PC and print management system, does not retain information on websites visited by customers. The Library reserves the right to limit workstation and printer usage at peak hours or to schedule workstation and printer use in order to*

accommodate the largest number of customers at specific agencies. ***--Pratt Library System (Maryland)***

*The Library does not monitor an individual's use of the Internet. Computer search stations are programmed to delete the history of a user's Internet session once the session is ended. The Computer Booking history is deleted every day. --**San Francisco Public Library (California)***

*Privacy screens are available for Internet computers. However, these screens cannot prevent other library users from seeing what you are viewing. The library's computers are in a public area. Others may be involuntarily exposed to what you are viewing. The library asks that you remain sensitive to the fact that you are working in a public environment shared by people of all ages. --**Multnomah County Public Library (Oregon)***

*Patrons may "lock" an Internet Station by pressing ctrl+alt+del and selecting "lock computer." Doing so allows a patron to leave a computer unattended without having his/her privacy compromised. To unlock the computer, the patron must press ctrl+alt+del again and re-enter his/her library card number and password. --**Multnomah County Public Library (Oregon)***

*As a courtesy to others, log off completely when you are finished with your session. This also protects the privacy of your search. To do this, press the Ctrl-Alt-Del keys, select Log Off, then Log Off again. --**Multnomah County Public Library (Oregon)***

Tips to Communicate Your Library Privacy Policy

As libraries continue to be a public access point for new technologies, the importance of patron privacy grows. Increasingly, libraries are developing policies around protecting patron privacy, as well as the limits of library staff in patron-technology interactions. It is important to ensure that patrons know how their privacy is being protected while using library technology and websites. However, possibly more important is empowering patrons to protect their own privacy while using publicly accessible technologies within the library. Through our library privacy policy framework, we hope to give library staff the tools for protecting patron privacy. But we also want to stress the importance of communicating these policies with patrons. Besides providing easy access to policies on the library system website, there are a number of ways library staff can communicate their library privacy policies, including but not limited to:

- Verbally alerting patrons to specific privacy policies when addressing an individual question/concern;
- Publicly posting privacy policies, preferably in the same location as library computers;
- Providing handouts with a summary of library privacy policies at various locations throughout the building;
- Creating an easily accessible link on the library homepage to navigate to library privacy policies;
- Sharing information about library privacy policies on social media and in email blasts; and,
- Providing written policies in English and the other languages commonly spoken by your patrons.

While the above is not an exhaustive list, it provides a starting point for communicating with patrons about evolving library privacy policies.

Disclaimer

The examples used in this framework were chosen to highlight various ways library systems in the U.S. are addressing the risks associated with patron data and technology use. Their inclusion does not denote an endorsement from the Safe Data Safe Family project.

Additional Resources for Crafting your Library Policy

Below, you'll find additional resources that should prove useful in crafting your library's privacy policies. This includes links to the library policies included in the examples and more information about the ALA Privacy Toolkit.

Links to Library Policies Used in this Document

The following links include some of the library privacy policies that were used to develop this privacy policy.

- Monterey Public Library (CA)
- San Francisco Public Library (CA)
- Santa Monica Public Library (CA)
- DC Public Library (DC)
- Pasco County Libraries (FL)
- Boise Public Library (ID)
- Ames Public Library (IA)
- Iowa City Public Library (IA)
- Acton Memorial Library (MA)
- Anne Arundel County (MD)
- Cecil County Public Library (MD)
- Enoch Pratt Free Library (MD)
- Montgomery County (MD)
- St. Mary's County (MD)
- South Thomastown Public Library (ME)
- Wayne Public Library (NJ)
- New York Public Library (NY)
- Cleveland Heights Public Library (OH)
- Multnomah County Public Library (OR)
- Dormont Public Library (PA)
- Eastern Monroe Public Library (PA)
- San Antonio Public Library (TX)
- Kitsap Regional Library (WA)
- Boulder Junction Public Library (WI)
- Madison Public Library (WI)

- Colorado Library Consortium Public Library Policy Collection - Established to provide small, rural libraries with EASY access to a clearinghouse of policies

Additional Resources About Patron Privacy

Disclaimer

The resources listed here are provided to aid you in your search for additional tools and information on how to protect patron privacy. Their inclusion is not an endorsement by our research team.

- OCLC is a global library cooperative that provides resources to the library community. The WebJunction Policies page offers examples of policies from a variety of libraries, as well as webinars such as this one on developing library policy.
- Library Records, Patron Privacy, and Library Policies is an article on the Public Libraries Online about developing library policies around patron privacy and library records.
- Library Freedom Project is an organization that provides librarians and their communities with privacy literacy resources, such as bookmarks with tips on protecting privacy and a guide for protecting yourself from online harassment.

ALA Privacy Toolkit

The ALA Privacy Toolkit provides several resources on how to develop a new privacy policy or update an existing policy. Resources like the Guidelines and Checklists are useful to ensure all areas of the library are covered in the library. Our privacy policy framework focuses specifically on library staff's interactions with patrons and covers many of the day-to-day privacy risks patrons face.