PRIVACY POLICIES

What is a Privacy Policy?

Privacy policies tell library users what data is collected about them, their data rights, and how that data is used, shared, stored, and deleted. These policies also give users information about third parties that have access to their personal information and direct users to vendor privacy policies. Well-written privacy policies give users clarity on how the library and its vendors handle their personal information and inform them about the laws that govern its use and disclosure.

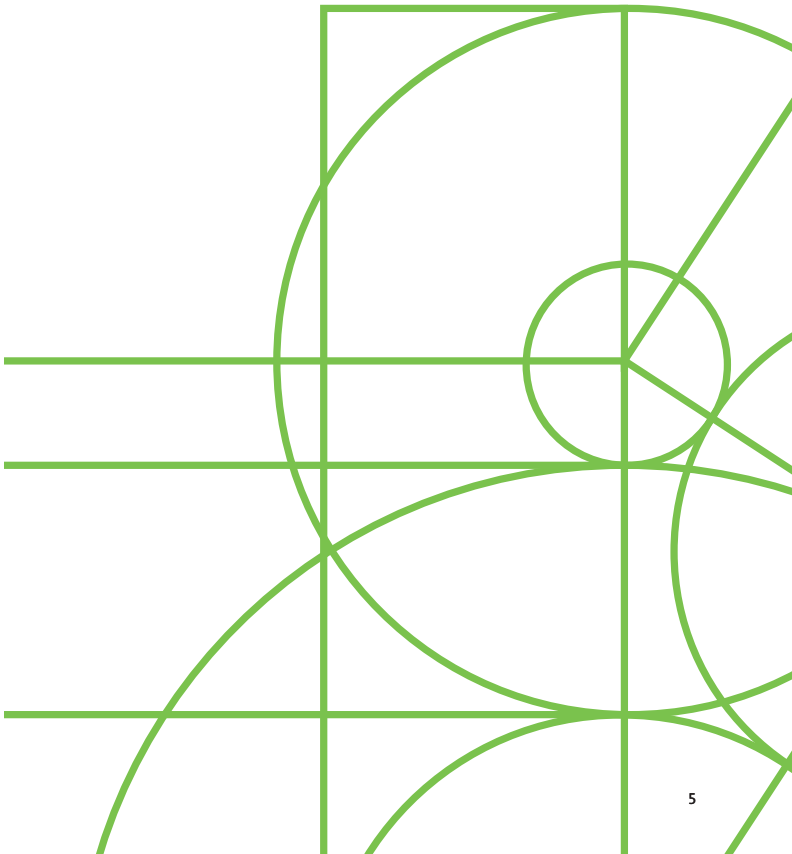
Not the decision maker or policy writer at your library? No worries! Use this guide to ask questions about vendor privacy policies and to advocate for your library to write its own policy. The "How to Talk About Privacy" Field Guide can help you have conversations with the stakeholders responsible for making changes.

Some school library workers may be unable to persuade decision makers to create and have the school board approve a privacy policy. Use this field guide to create an informal set of privacy guidelines and procedures that take into account state and federal laws as well as the Library Bill of Rights and Code of Ethics.

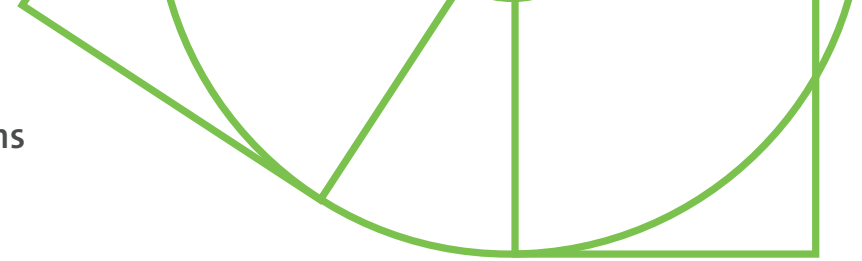
How to Read a Privacy Policy

Before we learn to write, we learn to read. The best writers are voracious readers, learning techniques and identifying pitfalls from the work of others. Privacy policies are notorious for being intentionally written to obfuscate (make unclear) rather than inform. They are written by lawyers to protect companies from litigation, not as a mechanism to aid in the understanding of the end user or to gain informed consent to use their information. By learning how to read privacy policies, you can start identifying when vendors have a privacy policy that aligns with your library's values and ethics. Reading privacy policies published by corporations will also teach you how to provide clarity in your own policies.

In this section you will learn about commonly used phrases and terms and policy red flags.



Understanding Commonly Used Phrases and Terms



"PERSONALLY IDENTIFIABLE INFORMATION" VS. "NON-PERSONAL INFORMATION"

- Personally Identifiable Information (PII) is information that can be used to identify a specific person. Some examples of PII include: name, Social Security number, birthdate, government issued ID number, financial account numbers, or contact information (email, phone number, address).
- Non-personal information will often include what operating system is being used, user analytics (what pages are visited or time spent on a page), device ID, and IP address.

"INFORMATION WE COLLECT" VS. "INFORMATION YOU GIVE TO US"

- In order to use a service, including the library, we often have to give over at least one piece of personal information. When someone signs up for a library card the information they give to us may include their name, address, and phone number. They are aware that this information was collected as they were part of the transaction.
- When an organization uses the phrase "Information We Collect" they are often talking about information that they gather without the user directly giving it to them. This may include a user's IP address, what operating system they're using, borrowing history, websites visited, search history, etc. Users are often unaware this information is being collected, and its collection is usually a condition of use. In a privacy policy, this information most often falls under the "non-personal information."

A piece of data that might be considered non-PII in one state or country could be considered PII in another based on local laws. Also, multiple pieces of data considered non-PII may still be used to identify someone.

"COOKIES"

Most privacy policies will talk about collecting cookies. These are small text files placed on a user's computer that collect personal data. This allows the website to recognize the user each time they return. Cookies can capture user settings, email addresses, and other personalization settings. It's important to know the difference between types of cookies so you can fully understand the privacy policy.

- Session or temporary cookies are only active while the user is browsing the site and are deleted when the browser is closed. For example, they may be used to retain items in a shopping cart.
- Permanent or persistent cookies remain active even after a browser has been closed. They may store a username, password, or personalization settings. Persistent cookies can also be used to track a user's interaction with the website.
- Third-party cookies are tracked by websites other than the one you are visiting and are most commonly used by advertisers and social media companies. They can track spending habits, online behavior, and demographics. If you've ever looked up something on one website and then saw advertisements for it on other sites you visited, it's because of third-party trackers.

"THIRD-PARTY"

- This often-vague term is used in most privacy policies. Many companies want to share at least some user data externally. A third-party entity might be used for data analytics, customer relationship management, or even advertising. Since library use data is protected to some degree by laws in most states, it is important to ask vendors what information is shared and with whom the information is shared including third-party entities. You might understand and feel confident in the data security practices of your vendor, but do you have that same confidence in a third party?

Hope you're hungry for more cookies! The cookies listed in this guide are just a few of the flavors available. To learn more about cookies, check out this guide from HTML.com http://bit.ly/MoreWebCookies

"AFFILIATED BUSINESSES"

- Many businesses have direct financial ties to other businesses. Two companies are considered affiliated when one is a minority shareholder of another. Privacy policies may state that user data is shared with "affiliated businesses." This is not usually considered selling user data, even though your library user's information may be shared with an outside entity you did not contract with. Ask vendors to disclose what information is being shared and with whom.

"COMBINE DATA" OR "DATA BROKER"

- Whenever we go online data is collected about us. This data could be everything from our shopping habits to what sites we frequent to which specific ads we've clicked on. Data brokers combine this data to create user profiles. Profiles are sold to other companies that allows them to send targeted marketing. If a vendor uses trackers or certain cookies, it's important to find out if that information is being compiled and shared with data brokers.

"OPT-IN" OR "OPT-OUT"

- The American Library Association's "Privacy: An Interpretation of the Library Bill of Rights," states "...users should have the choice to opt-in to any data collection that is not essential to library operations and the opportunity to opt-out again at any future time." Ideally, we want library users to have the choice when it comes to what data is collected and how it is used. If you see that a vendor's privacy policy has the default set to "opt-out," meaning the user has to manually choose to exclude themselves, ask them if it can be changed to reflect the library's commitment to privacy by making the default "opt-in."

"CONSENT" OR "EXPLICIT/ INFORMED CONSENT"

- Consent is a tricky concept online. Many websites say that they get a user's explicit or informed consent. However, that often just means ticking a box when registering for an account. A user is generally considered to have given their "regular" consent just by using the website. Most often, users have given their consent to a wide range of tracking just by opening up a website.

Red Flags

There are many commonly used phrases that should prompt you to ask your vendors questions about their practices. Some things you might not find as often in policies, but when you do see them they should immediately raise a red flag. When you find a red flag in a vendor's privacy policy, make a note and be sure to ask them to give you more details before entering into a contract.

SELLING/SHARING INFORMATION

- Any vendor should be able to explain the lifecycle of a user's data. If you see a privacy policy that mentions sharing data with fourth parties, ask for specifics. While you might trust the security and privacy practices of the vendor you're contracting with, do you know how this fourth party handles user data? Any mention of selling user data should be a huge red flag. Libraries already pay to access a vendor's platform; vendors should not also make money off of a user's data.
- **Example:** "Google uses the data collected to track and monitor the use of our Service. This data is shared with other Google services. Google may use the collected data to contextualise and personalise the ads of its own advertising network. You can opt-out of having made your activity on the Service available to Google Analytics by installing the Google Analytics opt-out browser add-on."

STORING/TRACKING LOCATION DATA

- Libraries and vendors should always strive to collect the least amount of data required to offer a service. Using GPS coordinates to target the exact location of a user can mean that person may be easily identified.
- **Example:** "When you access or use the Service, we may access, collect, monitor and/or remotely store 'location data', which may include GPS coordinates (e.g. latitude and/or longitude) or similar information regarding the location of your device. Location data may convey to us information about how you browse and use the Service. Some features of the site, particularly location-based services, may not function properly if use or availability of location data is impaired or disabled."

THIRD-PARTY INTEGRATIONS FOR USER AUTHENTICATION

- Many people like the convenience of using their Facebook, Google, or Microsoft account to log in to various services across the web. Sometimes these user authentication portals have embedded third-party trackers that give the platform access to a wide range of PII.
- **Example:** "We may receive information about you from third parties. For example, the Service may use Facebook or Google for user authentication. You should always review and, if necessary, adjust your privacy settings on third-party services before linking or connecting them to the Service."

CLEAR GIFS/WEB BEACONS/ TRACKING PIXELS

- These are transparent images embedded on websites and in emails. They are mostly used in conjunction with cookies and track user behavior across the web. They can be used in emails to notify the sender when a recipient has opened a message. Web Beacons cannot be denied or blocked like cookies. The most pervasive of them can even give over specific location data.
- **Example:** "We use pixels to learn more about your interactions with email content or web content, such as whether you interacted with ads or posts. Pixels can also enable us and third parties to place cookies on your browser."

EMAIL COMMUNICATION (SIGNING PEOPLE UP FOR MARKETING EMAILS)

- The ideal setup for a user to access a vendor's product through the library would be where they do not need to share their email to create an account. Their library card number and PIN should be sufficient. When this is unavoidable, it is important that the vendor use the email address sparingly and not push advertising messages to the user.
- **Example:** "We will contact you through email, mobile phone, notices posted on our websites or apps, and other ways through our Services, including text messages and push notifications."

DISCLOSURE OF INFORMATION

- Vendors may get requests from law enforcement to disclose user data. This is part of the reason we want vendors to collect the least amount of information possible. It is reasonable to see a notice in a privacy policy that states that a user's information may be shared with law enforcement, but the vendor's ability to release users' information should be limited in scope. Seek to add contractual language that requires a vendor to notify the library when a request to disclose information is made and to only release users' information when compelled by law.
- **Example:** "Regardless of the choices you make regarding your information and to the extent permitted or required by applicable law, we may disclose information about you to third parties to: (i) enforce or apply this Privacy Policy or the Service Terms; (ii) comply with laws, subpoenas, warrants, court orders, legal processes or requests of government or law enforcement officials; (iii) protect our rights, reputation, safety or property, or that of our users or others; (iv) protect against legal liability; (v) establish or exercise our rights to defend against legal claims; or (vi) investigate, prevent or take action regarding known or suspected illegal activities; fraud; our rights, reputation, safety or property, or those of our users or others; violation of the Service Terms; or as otherwise required by law."

OWNERSHIP OF DATA

- The details around ownership of data can usually be found in the vendor contract. What you're looking for in a privacy policy is language that describes what happens to that data if a company is bought, sold, or transferred. A library should not be forced to share its user data with a new company until they have had the opportunity to enter into a new contract. Keep an eye out to see if the privacy policy clearly states if the library or its users have ownership over the data they provide directly to the vendor. Library user data should never be allowed to become a business asset of the vendor.
- **Example:** "In the event that a division, a product or all of Company is bought, sold or otherwise transferred, or is in the process of a potential transaction, personal information will likely be shared for evaluation purposes and included among the transferred business assets, subject to client contractual requirements and applicable law."

SECURITY

- While there are no 100% guarantees that user data can be secured, when a privacy policy uses soft language (e.g., may, try, might, etc.) or calls out their inability to secure user data, it is a red flag. This language is used to absolve the company of legal responsibility should a breach occur. Look for privacy policies that tell you how they secure the data, not that they are likely unable to do so.
- **Example:** "The security of your data is important to us but remember that no method of transmission over the Internet or method of electronic storage is 100% secure. While we strive to use commercially acceptable means to protect your Personal Data, we cannot guarantee its absolute security."

EXERCISE

Scavenger Hunt!

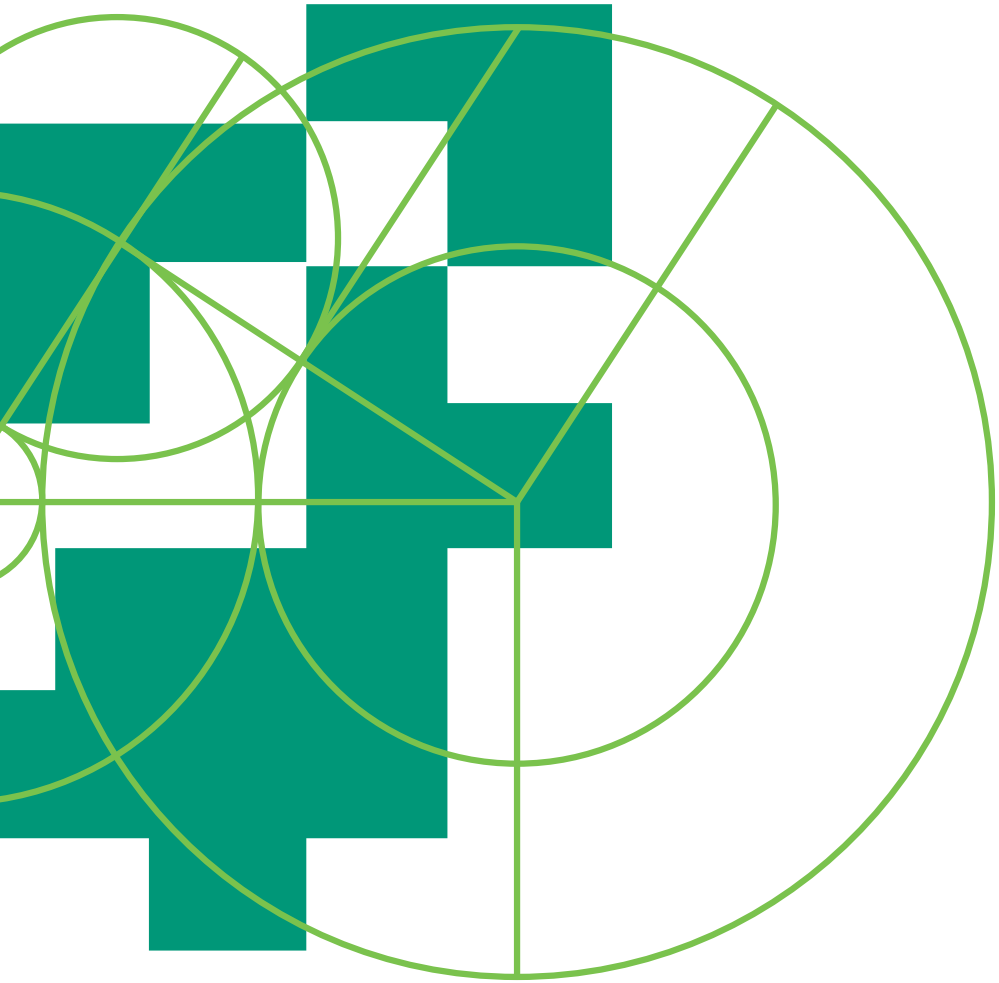
Locate the privacy policy from at least one of your library vendors. Read through the policy and compare it with the red flag and commonly used phrases lists in this guide.

- **What vendor policy did you look at?**
- **What red flags did you find?**
- **What other red flags not listed did you discover?**
- **What else did you find that you didn't understand?**
- Take these red flags to your vendor (or library worker that is responsible for vendor products) and ask for clarity.

How to Write a Privacy Policy

Writing in Plain Language

The Plain Writing Act became law in 2010, requiring federal agencies to use clear government communication that the public can easily understand. As we know from reading all those privacy policies, not many of them are written in plain language. By learning the principles of plain writing, you can craft a privacy policy for your library that your users will quickly understand.



EXERCISE

Visit the Plain Language website (http://bit.ly/UsePlainLanguage) and review all of the guidelines. You will find information on how to:

- Write for your audience
- Organize the information
- Choose your words carefully
- Be concise
- Keep it conversational
- Design for reading
- Follow web standards
- Test your assumptions

*The information and exercises found in this section comes from https://www.plainlanguage.gov/

PLAIN LANGUAGE TIPS

Be conversational and use pronouns to speak directly to your reader: "We care about your privacy" not "The New Town Library cares about your privacy"

Add useful headings: "What information do we collect?"

Be concise and descriptive

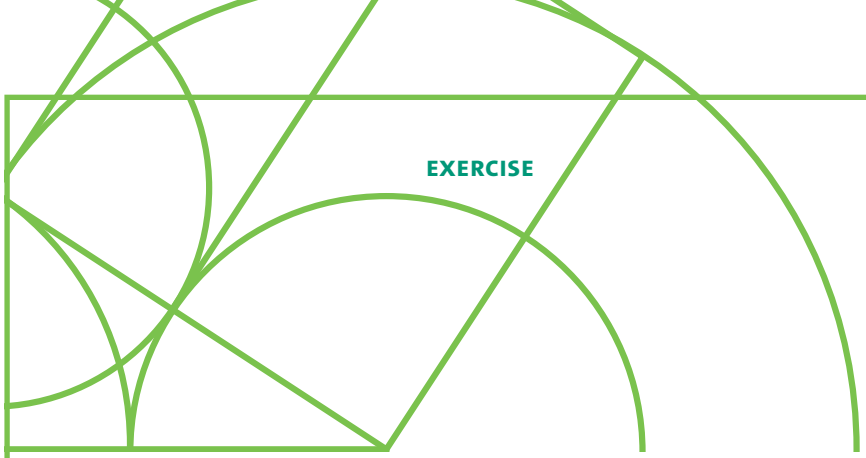
Avoid jargon and minimize abbreviations

EXERCISE

Understanding your audience is the first step in writing your policy. You need to understand who will be reading so that you can write for them. A privacy policy written for third-grade students at an elementary school library will look different from the one written for college students at a university. However, any policy should be written in plain language that delivers your message clearly.

Consider your privacy policy and answer the following questions:

- Who is my audience?
- What does my audience need to know?
- What's the best outcome for my library? What do I need to say to get this outcome?

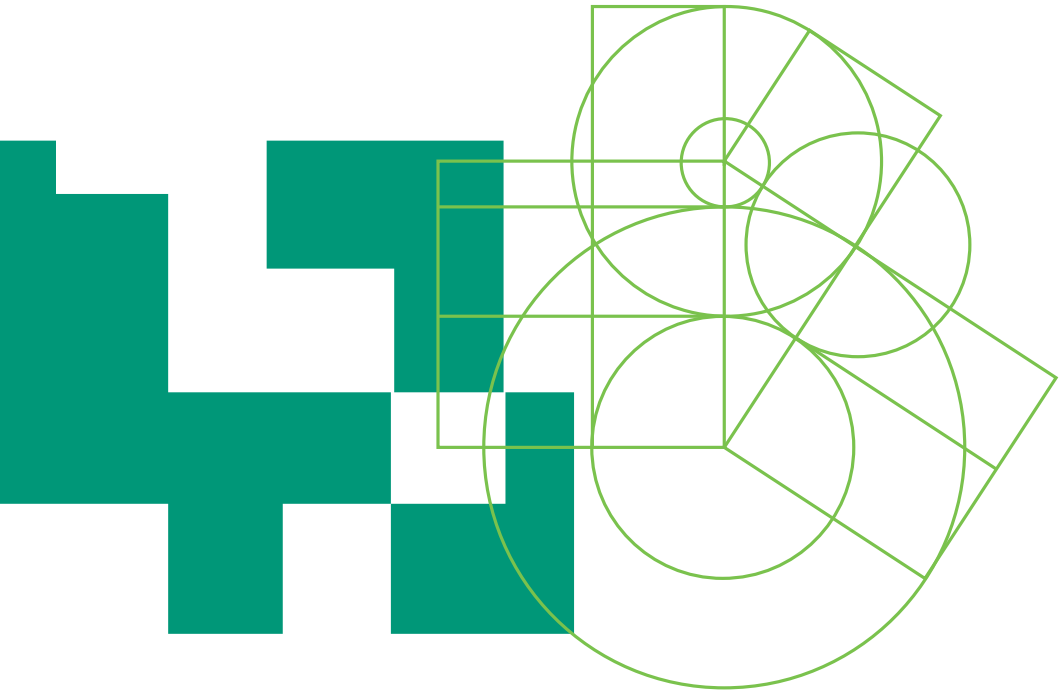


EXERCISE

- What does my audience already know about library privacy?
- What questions will my audience have?
- What's the best outcome for our audience? What do I need to say to get this outcome?

Writing Your Privacy Policy

There are several key areas to include in any privacy policy. There is no need to reinvent the wheel! The Library Freedom Institute has created a template for any library to use when crafting their policy (http://bit.ly/LFIprivacytemp). Review the template. What phrases or sections resonate with your library's practices? What language can you use in your policy? All library policies should be reviewed and approved by the governing board and legal counsel before being implemented.



Check out these library privacy policies for other wording suggestions.

- http://bit.ly/SJPLPrivacyPolicy
- http://bit.ly/MultPrivacyPolicy
- http://bit.ly/CornellPrivacyPolicy
- http://bit.ly/RutgersPrivacyPolicy

EXERCISE

Complete each section in this exercise to start drafting your privacy policy.

PRIVACY STATEMENT - YOUR RIGHT TO PRIVACY

This is the section where you can tell users why privacy matters to libraries. Write details about your commitment to privacy values and ethics. Include links to applicable local, state, and federal laws.

WHAT INFORMATION DO WE COLLECT?

Users have the right to know every type of information that is collected by the library. Include any and all PII and non-personally identifiable information you might collect. This section should also include information collected as part of any kind of analytics program. Including a link to third-party vendors' privacy policies is helpful here. Be sure to include information that may be collected through email, chat services, RFID, or any reference interactions.

This is a good section to include your retention policies. Let users know how long you keep any information, including their borrowing history. If you have a written retention policy, provide the link.

WHO HAS ACCESS TO MY INFORMATION?

Remind users that their information is confidential, but also tell them who has access to it at your library. This is a good place to discuss policies around one user getting access to another user's information (e.g. a parent asking for their child's records).

EXERCISE

HOW DO WE PROTECT THE PRIVACY OF STUDENTS AND MINORS?

Many libraries serve users that may have specific privacy rights under local, state, and federal law. If you serve students or minors, be sure to address how your library protects their privacy.

OUR WEBSITE AND PUBLIC COMPUTERS

This might feel like the most complicated section if you're unfamiliar with technology. If possible, seek out help from the Information Technology department to fill out the details in each of these sections.

- **HTTPS**
  Let users know what HTTPS is (it's a certificate that encrypts your network traffic) and that your library employs it on your website.

Does your library lack a secure website? Get a free SSL certificate with Let's Encrypt http://bit.ly/LibLetsEncrypt

EXERCISE

- **Cookies**
  Explain what cookies are (see the commonly used term section in this guide) and let users know what cookies your site uses. This section is likely to mostly be teaching users about cookies.

- **Data and Network Security**
  Let users know that you are actively working to prevent their data from getting into the wrong hands. You don't need to go into elaborate detail here, but avoid using phrases found in the red flag section like, "we may protect your data" or "reasonable measures."

- **Public Computers and Connected Devices**
  If your library offers WiFi access, device checkout, or pubic computers, here is where you can tell them what protections are in place. Let users know how long you keep a log of their computer usage (hopefully not more than 24 hours) and what happens to their data when they log out of a computer or return a device.

EXERCISE

THIRD-PARTY VENDORS

Most library users think anything they access from the library's website is part of the library. They don't have knowledge of the vast third-party vendor network. In this section give a summary of the types of information that may be collected, used, and shared by these vendors. Provide a link to an easy-to-read and regularly updated page that has links to all of the third-party vendor privacy policies. Also, include what the library's expectations are for vendors. This information may be included in the contracts or requests for purchase.

WHAT SURVEILLANCE IS USED IN THE LIBRARY?

Many libraries employ some form of surveillance. Be upfront and honest with your users. Include details on security cameras and any body-worn cameras (including retention policies and who has access to the footage), facial recognition software, and smart speakers.

EXERCISE

HOW DO WE HANDLE REQUESTS FROM LAW ENFORCEMENT?

Detail the procedures in place when a request from law enforcement comes in to access a user's records. Include information about any training staff has undergone.

Congratulations! You've just completed the first draft of your library privacy policy.

Put your answers to these questions into one document and include the section headings.

Your library may also want to include a transparency report as part of its privacy policy. A report would provide the number of requests made, what agencies requested information, and how many requests were fulfilled. Check out Google's Transparency Report for an example: http://bit.ly/GooTransparency

ALA American Library Association

PRIVACY ADVOCACY GUIDES

Privacy is a core value of librarianship, yet it often feels like an overwhelming and onerous undertaking. Use these Privacy Field Guides to start addressing privacy issues at your library. Each guide provides hands-on exercises for libraries. Check out all the available guides at **bit.ly/PrivacyFieldGuides.**

INSTITUTE of Museum and Library SERVICES

This project was made possible in part by the Institute of Museum and Library Services LG-36-19-0073-19.

Designed by PixelbyInch.com