What is a Privacy Audit?

Privacy audits are procedures to ensure that your organization's goals and promises of privacy and confidentiality are supported by its practices, thereby protecting confidential information from abuse and the organization from liability and public relations problems.

A privacy audit provides a library an opportunity to examine:

- How privacy matters are handled at all levels

- The flow and storage of data

- The role data plays within the organization

- Staff training about privacy matters

- Existing and needed privacy policies

- User privacy and confidentiality

This is an ongoing process, not a one-shot project. Audits will look different depending on the size of the library and the level of control staff have over their technology infrastructure.

Why are Privacy Audits Important?

Privacy is essential to the exercise of free speech, free thought, and free association. It is the responsibility of all libraries to ensure that their procedures and policies are designed with privacy in mind. If users lose their privacy, then they lose what makes a library so great: that freedom to seek information without fear of reprisal. It is the responsibility of all libraries to ensure that their procedures and policies are designed with privacy in mind.

In today's society, there is almost no place a person can go to seek out information without being tracked. Libraries have an ethical and democratic duty to be that place. When people are being watched, they change their behavior. A library that monitors and shares a user's information is no longer protecting intellectual freedom. Libraries should make every effort to provide a private place for people to exercise their information access rights by performing regular privacy audits.

Every library needs to perform audits to understand how they, their vendors, partners, and administrators are handling user data. Even if your library is one room with one person on staff you can ask the core set of audit questions. Understanding what current practices are is the first step in crafting privacy-minded procedures and policies. With an increased reliance on third-party vendors, libraries are not able to have full control over users' data. However, a privacy audit will assist libraries in being transparent with users about how
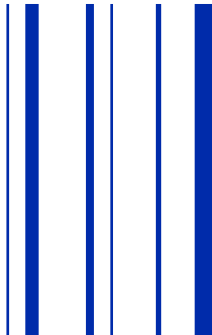
Building the Audit Framework

A privacy audit will cover a wide breadth of information, allowing you to dig
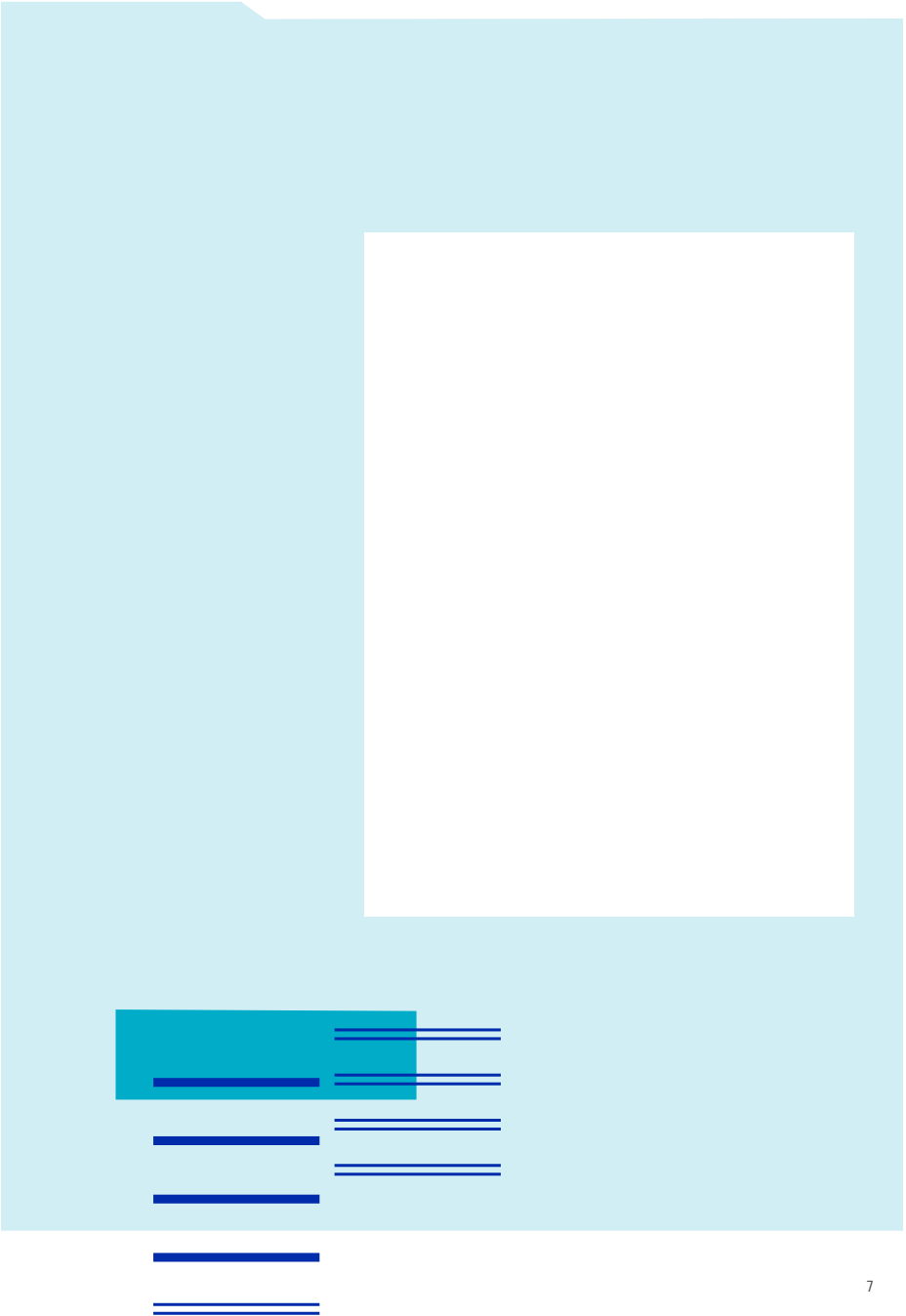
Core Questions

Once you've identified all the areas in the library that interact with user data, you'll want to ask yourself a set of Core Questions. Keep these questions handy and ask them anytime you, a partner, or a vendor is planning to collect user data. They will help you to collect the least amount of data needed, ensure it's stored securely, and deleted according to a regular schedule.

EXERCISE

Pick one of the places in your library that collects user data. Answer these Core Questions.

- What information do you collect?

- Why do you collect it? Do you need to collect it?

- How do you collect it?

- Who has access?

- What are the storage and retention policies/procedures?

- What are the current best practices and policies?

Is the user data shared with or collected by third-party vendors?

- What vendors are used?

- What information is shared or collected by the vendor?

- Is the information collected by the vendor necessary for business operations?

- What are the vendor's privacy policies and do they align with the library's?

- What changes need to be made to ensure the privacy and security of user data?

Using Guidelines and Checklists

The Core Questions are a great starting place for any audit. The next step is to dig in deeper and align your library with the privacy guidelines established by the American Library Association (ALA). ALA has created a set of guidelines and checklists that are available to assist librarians, libraries, schools, and vendors to develop best practices for online privacy, data management, and security.

The guidelines and checklists were created for every library, of any size, to be able to use. The checklists are broken down into three priority levels.

- **Priority 1** items should be achievable by every library. These are the must do items.
- **Priority 2** items will be able to be met by larger systems and those with more control over their IT systems.
- **Priority 3** are for those libraries with a deeper technological understanding and resources. Some of these will be optional.

You can use these checklists as part of the audit process. They will enable your library to be in alignment with the ALA guidelines and give you insight about current practices and policies.
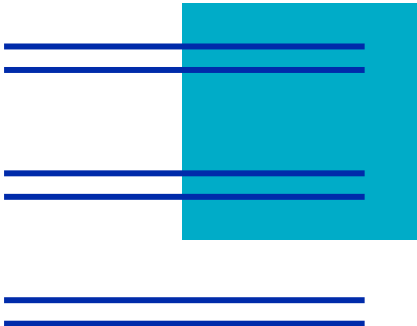
EXERCISE

Complete the Privacy Checklist Overview. As you complete the checklist, ask yourself, "Is our library already doing this?" or, "Is our library doing this, but it needs work?" or if you're not doing it all, "What does our library need to do in order to complete this checklist item and who's going to do it?".

PRIVACY CHECKLIST OVERVIEW	STATUS	STAFF ASSIGNED	DUE DATE	NOTES
Create a privacy policy that addresses the collection of user information. For guidance see the Privacy Policies Field Guide.	NOT STARTED IN PROGRESS NEEDS WORK COMPLETED			
Destroy all paper records with user data that no longer have a business need, such as computer sign-in sheets. Keep any future records in a secure location.	NOT STARTED IN PROGRESS NEEDS WORK COMPLETED			
Ensure all existing security certi cates for HTTPS/SSL are valid and create a procedure				

Performing the Audit

Telling the Audit Story

If you are at a larger library you will want to establish a team to complete the audit. Smaller libraries may nd themselves with a team of one. That's okay! Even if you don't have the ability to make large sweeping changes, plan to audit whatever you can. Ask those Core Questions and identify the areas where you can make changes

An audit doesn't just happen in someone's head as they think about all those questions and checklist items. Y
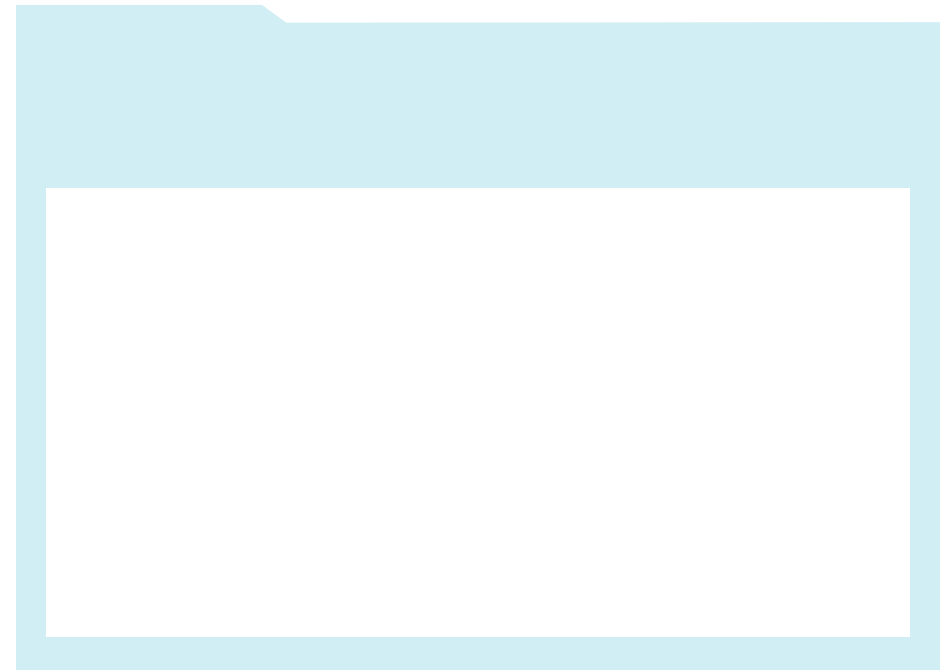
EXERCISE

- **Create spreadsheets for each of the ALA Privacy Checklists.** Only add the items from the priority level that your library is following. Also, create documents where you can answer the Core Questions for each of the areas of your library that handle user data.

- **Assign tasks.** Establish who will be responsible for seeing if the library is currently in compliance with a checklist item. Will that same person be responsible for bringing you into compliance? Identify who will research and document the answers to the Core Questions.

- **Build a timeline.** Create due dates for completing checklist items and answering Core Questions. If changes need to be made, when do they need to be completed?

- **Document your ndings.** Everything you audit should have a document that outlines your ndings. If you discovered changes that need to be made, determine who has the authority to change them. Bring your documentation to the appropriate sta to make a case for new policies and procedures.

You may have to interact with units outside of the library such as campus or school IT. Set up a meeting to discuss the audit. Do they already perform one regularly? Can the ALA checklist items be added to their audit process?

Rinse and Repeat!

Your first privacy audit will be the most challenging and require the most work.