



THE ULTIMATE
**PRIVACY
FIELD
GUIDE**

A WORKBOOK OF BEST PRACTICES

EDITED BY ERIN BERMAN AND BONNIE TIJERINA
ALA OFFICE FOR INTELLECTUAL FREEDOM (OIF)

ALA
Editions
CHICAGO 2023

alastore.ala.org

ERIN BERMAN is a fierce privacy advocate who led the Privacy Subcommittee of ALA's Office for Intellectual Freedom from 2018 to 2022. During her time as innovations manager for the San José Public Library, she published the book *Your Technology Outreach Adventure: Tools for Human-Centered Problem Solving*. Currently, she works as the division director of the Learning Group for the Alameda County Library in California.

BONNIE TIJERINA is a researcher, librarian, and community convener. She is currently focused on creating opportunities for education and discussion in the library profession and beyond on the role libraries and librarians can play in the increasingly complex issues of the digital world. In that space, she has worked on several grant-funded projects that involve privacy and big data research ethics, and she is the coeditor of *Protecting Patron Privacy: A LITA Guide*. She is also the founder and annual coordinator of the Electronic Resources & Libraries Conference.

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

© 2023 by the American Library Association

Extensive effort has gone into ensuring the reliability of the information in this book; however, the publisher makes no warranty, express or implied, with respect to the material contained herein.

ISBN: 978-0-8389-3730-3 (paper)

Library of Congress Cataloging-in-Publication Data

Names: Berman, Erin, editor. | Tijerina, Bonnie, editor.

Title: The ultimate privacy field guide : a workbook of best practices / edited by Erin Berman and Bonnie Tijerina, Office for Intellectual Freedom.

Description: Chicago : American Library Association—ALA Editions, [2023] | Includes bibliographical references and index. | Summary: "Designed for use in school, public, and academic settings of all shapes and sizes, this easy-to-use workbook is packed with practical, hands-on exercises to guide you towards creating a more privacy-focused library"—Provided by publisher.

Identifiers: LCCN 2022029484 | ISBN 9780838937303 (paperback)

Subjects: LCSH: Privacy, Right of. | Intellectual freedom.

Classification: LCC JC596 .U57 2023 | DDC 323.44/8—dc23/eng/20220729

LC record available at <https://lcn.loc.gov/2022029484>

Original design by Heejung Yoon, Ryan Carnrick at PixelbyInch.com.

Layout adapted by Kim Hudgins.

© This paper meets the requirements of ANSI/NISO Z39.48-1992 (Permanence of Paper).

Printed in the United States of America

27 26 25 24 23 5 4 3 2 1

CONTENTS

	<i>Acknowledgments</i>	<i>vii</i>
	<i>Introduction</i>	<i>ix</i>
1	Digital Security Basics	1
2	How to Talk About Privacy	11
3	Non-Tech Privacy	21
4	Data Lifecycles	33
5	Privacy Audits	43
6	Privacy Policies	53
7	Vendors and Privacy	69
	<i>Index</i>	<i>83</i>

INTRODUCTION

With the creation of ever larger datasets and methods to track users' every movement online, library workers need to have a deep understanding of privacy, confidentiality, and security. While privacy is a core value of librarianship, it often feels like an overwhelming and onerous undertaking. Library workers need easy-to-use tools that will help them create private and secure spaces for users to express their intellectual freedom.

The editors of this book, Bonnie Tijerina and Erin Berman, saw that there was a lack of practical how-to guides for making concrete privacy changes in the library. As a librarian and researcher, Bonnie has focused on the role libraries play in supporting their communities in the digital space. As an active member and then chair of the Privacy Subcommittee of ALA's Office for Intellectual Freedom, Erin has heard often from library workers who feel passionately about supporting users' privacy rights but feel unprepared, not tech-savvy enough, or not in the right position of leadership to make a change.

To address the concerns voiced by library workers, Bonnie and Erin partnered to create the "Privacy Field Guides." Sponsored by the Institute of Museum and Library Services and the American Library Association, these short online guides are designed to work in school, public, and academic libraries, making it easier to talk about privacy and take steps, even small steps, to improve the library's or its users' privacy in some way.

This publication gathers those guides together into one workbook, with each chapter representing a guide that covers topics important to library workers, including the basics of digital security, understanding the data lifecycle, performing library privacy audits, and writing or reading privacy policies. The chapters also help libraries learn how to talk about privacy with stakeholders, how to work with vendors to secure privacy requirements, and what to consider around nontechnical privacy issues.

This workbook has been thoroughly reviewed and then vetted in real-world library settings. Library stakeholders from across the country participated in surveys, trainings, workshops, and focus groups to provide input and guidance about the content and format of these guides. Library privacy experts wrote the guides, which were then put through real-world testing before reaching their final versions.

The workbook chapters are structured to give library workers the tools they need to create and be advocates for a safer, more secure library. Each chapter will give an introduction to the topic and then provide several exercises for you to implement privacy changes at your library. Each chapter follows the same easy-to-use format. You can read this workbook cover to cover, but we imagine you will choose a chapter that interests you or is in an area that your library would like to work on. Then you can revisit this workbook several times to learn about other aspects of privacy.

While some of the work in these chapters may not seem like big steps, these small but consistent actions can have large implications for your community. Learning the language to advocate for privacy, tweaking physical spaces, using new digital security tools, rethinking policies and practices, and asking questions within your organization will make a difference. With many libraries taking these steps, there is the possibility for powerful, collective change.

Digital Security Basics

Understanding basic digital security concepts, and knowing where to go for more help, is a great first step for all who work in libraries. Not only will these skills help make the library and its data more secure, but they will also allow staff to better help users to be more secure online. This chapter is intended for individuals who want to learn digital security skills and for those hoping to provide privacy and digital security education for library staff.

In This Chapter

Creating Strong, Secure Passwords	2
Passwords Are Out, Passphrases Are In	2
Password Managers	3
Multi-Factor Authentication	3
Phishing	4
Malware = Malicious Software	6
Ransomware	6
Network Privacy	7
Staff and User Training	8
Digital Security Detective	9



Creating Strong, Secure Passwords

Do you lock your house when you leave for the day? Most of us probably would answer “yes” to this question. Why do we secure the door? We lock our homes because we have things inside that we don’t want anyone else to have access to or steal. Creating a strong password is like having a unique key and lock to your house. We have to make sure that those locks are strong!

Passwords Are Out, Passphrases Are In

Remembering passwords for eighty different accounts is a challenge. We want to have a unique password for every account, and this can get out of control quickly. How can a person be expected to come up with a secure password that can also be remembered? Passphrases!

EXERCISE

Practice making a passphrase. The strongest passphrases will have at least seventeen characters (and spaces count).

1. Think of a set of words that have meaning to you and that you’ll remember. Do not include any personal information such as birthdates, addresses, or names. String together a combination of these words to create a random phrase.
2. Add numbers and symbols to the phrase at the beginning, middle, or end.
3. Now, test your passphrase (<https://howsecureismypassword.net>) and see how quickly it can be broken.

QUICK TIP

Forget about replacing “i” with “1” or “for” with “4.” These techniques are so common now that the computer programs that crack passwords know them too.

Password Managers

TRY A PASSWORD MANAGER

Dashlane:
dashlane.com

1password:
1password.com

LastPass:
lastpass.com

How many passwords are you expected to remember at work? Do you have them written down on a sticky note that's placed "discreetly" under your keyboard or in an office drawer? Believe it or not, one of the most common ways hackers gain access to accounts is through the person responsible for keeping their accounts safe. One solution to too many passwords is using a password manager.

Password managers generate and store complex passwords for you. You just have to remember one (very secure and unique) master password for the manager itself, and everything else is taken care of for you. Also, organizations can utilize a team password manager to manage shared accounts.

- Explore the password manager suggestions in this chapter. Then set up an account and try it out for a week.
- Use your strongest passphrase as the password for your password manager.

Multi-Factor Authentication

QUICK TIP

Are you saving your passwords with your browser? Watch out. This is not secure and is easily hacked. Password managers make it much harder for anyone to access your complex passwords and phrases.

For accounts that hold a lot of our personal information, we want to make sure we're the only ones with access. *Multi-factor authentication* (MFA) means that just entering a password on the computer isn't enough for someone to gain access to your account. The term *2-factor authentication* is commonly used as well, and is a subset of MFA that only requires one additional factor in addition to your password to grant access.

With MFA, when you enter a password into a digital account, you will be prompted to verify your identity through another means. Most often you will be texted a code to the phone number on file. That code would then need to be entered into the account to gain access. Sometimes MFA will utilize an authorization app, use a physical object like a security token, or request a biometric identifier.

If you ever see one of these texts come to you when you're not trying to access the account, then you know someone else is attempting to break in. This is a good time to change your password.



EXERCISE

- Review your personal accounts and enable MFA where possible. In the table below, list the current accounts you have, whether or not they have multi-factor authentication, and if they do, what that verification involves.

ACCOUNT	MULTI-FACTOR AUTHENTICATION (Y/N)
<i>Email</i>	<i>Y - password, text code, second email verification, phone call</i>

- Multi-factor authentication can also be used at the library. Can you think of any accounts that could benefit from adding multi-factor authentication?

Phishing

Phishing is the practice of sending fraudulent e-mails that claim to be from reputable sources to trick users into revealing personal information that can then be used for illicit or malicious purposes. Most libraries have filtering software for their e-mail accounts, but this doesn't mean you shouldn't be on the lookout for phishing e-mails.



Avoid Getting Caught

QUICK TIP

If you have clicked on a link you think might be malicious, let your IT staff know right away.

- Only click links in e-mail from trusted sources.
- Don't download an attachment unless you know who it's from.
- Don't enter your personal information into any form you have reason not to trust.
- Use context clues and listen to your gut. Just because an e-mail looks like it's from a coworker doesn't guarantee that it is. A hacker can send a message that appears to be from your coworker by hacking or spoofing their e-mail address.
- Look at the entire URL you are being asked to click on. Is it exactly the same as the site address you normally type?

Example of a Phishing Scam

RP Rachael Prestrio <president973@aol.com>
Today, 9:55 AM
Kelly, Are you free at the moment?
Regards
Rachael Prestrio | Libary Staff

Wilson, Kelly
Today, 2:09 PM
Do you still want to talk?
Sorry, I was in meeting.
Kelly Wilson | Manager, Twin Peaks Public Library

RP Rachael Prestrio <president973@aol.com>
Today, 2:15 AM
Yeah i just need you to do something for me. I am tied up right now, can you purchase Itunes gift card 3 pieces - \$100 each? I would reimburse you when am through. If you go to this site you can purchase the girft cards <https://itunes.gcardbonza.ltd/?=539s4>. Let me know!
Regards
Rachael Prestrio | Libary Staff

Q: What are the phishing red flags in this e-mail between employees at different libraries?

- A:**
- The e-mail domain is from AOL. This is not a typical domain used by libraries.
 - The response e-mail asked for money.
 - There are several typos.
 - The recipient is asked to visit a link and provide personal information.

Malware = Malicious Software

Malicious software is software designed to do damage or other unwanted actions to your computer or smartphone. Usually this type of software is installed on your computer when you download attachments in e-mails or click on unknown links or ads. It can also be installed when someone puts an external flash drive into your machine. If you open an e-mail and don't know what the attachment is, don't download it!

QUICK TIP

Check to see if your work or personal e-mail has been compromised by going to <https://haveibeenpwned.com>.

Activities to Secure the Library Workplace

- Check if your computers have antivirus software installed on them. Do the computers for users have the same protections as staff computers?
- Check to see if your mobile devices are updated to the latest version of the operating system (OS) they use.
- Create a schedule to regularly update the OS and software when updates are released, as malware can exploit security holes. You should check computers and all mobile devices.
- Does your library allow the use of external flash drives? Create procedures that do not allow staff to put external flash drives from users into staff terminals.

Ransomware

One type of malware gaining in popularity is ransomware. How does it work?

Attackers gain access to your computer when you accidentally download malware, and then they hold your information hostage. The attackers may lock all your files or shut down your entire network, and they will require you to pay them to regain access. If files are important to you, make sure to back them up to external drives or a cloud server.

These attacks often focus on businesses and governments so watch out for suspicious e-mails at work. If it feels wrong, report it to your IT department. If you see a suspicious e-mail in your personal account, mark it as spam (if possible) and delete the e-mail without clicking on anything.

QUICK TIP

Regularly update your devices. Updates are often security patches. Your apps and software are only protected when you're running the latest version of them.

EXERCISE

1. Perform a search for news reports of ransomware attacks on libraries. How many libraries can you find that have experienced attacks?

2. Does your library have a plan in place for a ransomware attack? Connect with your IT department and ask them the questions below. If no plan exists, try to develop one.

- How will staff be contacted without access to e-mail?
- How will users be notified of a ransomware attack?
- Does the library have a method for users to check out materials without access to the ILS?

Network Privacy

Pull up your library website. Look in the address bar. Do you see a little lock that's closed or open? Does your web address say HTTP or HTTPS? The "S" at the end of HTTPS stands for "Secure." It means that all communications between your browser and the website are encrypted, so no one else can see the data that is being sent.

It is very important that your library website use HTTPS (rather than just HTTP), especially on the accounts page. People visiting your site without HTTPS may even get warnings from their browsers telling them your site is not secure.

Getting Your Website to HTTPS

How can you move your library's website from HTTP to the HTTPS protocol? First, connect with your IT manager, or get ready to start the process yourself if you're the one with network access. Seek out the options for purchasing certificates for either SSL or TLS—the two standard security technologies that are used in HTTPS. If costs are a concern, check out Let's Encrypt (<https://letsencrypt.org>). Let's Encrypt offers free certificates to anyone who owns a domain name. There is a robust community of support available to help install the certificates and get your site secured.

EXERCISE

1. Go to your library's website. Is it secured with HTTPS?
2. If your site is still operating with HTTP, connect with the IT department or get ready to start the process if you're the one with network access. Seek out options for purchasing SSL/TLS certifications.
3. If your site is secured, visit a few library vendors to see if their sites are secure.

Staff and User Training

Once you understand the basics, it's time to share that knowledge in your library. When thinking about staff training, consider the following:

- How to get staff buy-in. Explain to your staff why privacy is important and vital to library operations.
- How to upgrade the technical skills of your staff with regard to digital security and privacy. Start out with the basics. This chapter is meant to support all staff members, including those who are less tech-savvy.
- Consider ways to measure improvements after training and ways to keep the conversation going.

Even a short staff development session with the topics above will make the library, the staff, and your users safer. Use the lessons and activities from this chapter to host a staff or user training session. You can also use library privacy and security training materials that are available online. You can find all of the following resources at www.ala.org/advocacy/privacy/training:

- Staff training resources from NYC Digital Safety: Privacy and Security, the Data Privacy Project, and the Library Freedom Institute
- Programming for students at academic libraries
- User programming for public libraries
- Lesson plans for students at K–12 libraries



INDEX

- A**
AASL (American Association of School Librarians), 31
academic libraries
 overdue items in, 26
 user privacy protection, 39
access
 in library privacy policy, 66
 in Library User Data Lifecycle, 38–39
acquisitions, 70–71
advocacy
 library privacy advocacy, 18–19
 relationships for, 20
“affiliated businesses” phrase, 56
aggregated metrics, 71
American Association of School Librarians (AASL), 31
American Library Association (ALA)
 Code of Ethics/Bill of Rights on user privacy, 28–29
 on opt-in choice for privacy policy, 57
 “Privacy Field Guides” sponsored by, ix
 privacy guidelines/checklists, 48–49, 50
 resources for law enforcement requests, 39
annual audit, 39
antivirus software, 6
APIs (application programming interfaces), 79
apps, 79
arguments, persuasive, 17
attachment
 malware from, 6
 phishing scam from, 5
audience
 determination of, 12
 empathy map exercise, 13–14
 persuasive arguments, creating, 17
 for privacy policy, exercise for, 62–63
audits
 annual audit of access levels, 39
 vendor audits, 79–80
 See also privacy audits
authentication
 multi-factor authentication, 3–4
 third-party integrations for user authentication, 58
- B**
Berman, Erin, ix–x
best practices, 48
bias, 15
browser
 cookies and, 55–56
 saving passwords with, 3
- C**
cameras
 in library privacy policy, 68
 user surveillance in library, 24
case studies
 on anonymizing holds, 29–30
 on library privacy advocacy, 19
catalog, 31–32
checklists
 ALA’s privacy checklists, 50
 for privacy audit, 48
children
 access to child’s library records, 19
 private spaces in library for, 22
 right to privacy, 15
Code of Ethics (American Library Association), 28–29
collection
 of data by third-party vendors, 67
 information given vs. information collected, 55
 in Library User Data Lifecycle, 34–36
 in privacy policy, 65
collective voice, 18
“combine data,” 57
communication, about privacy
 audience, determination of, 12–14
 case studies, 19
 general talking points, 14–15
 introduction to, 11
 library privacy advocacy, 18
 organizational culture and, 20
 persuasive arguments, creating, 17
 privacy point, getting across, 15–16
computers
 malware security for, 6
 privacy policy on, 66–67
 private spaces in library for, 22–23
confidentiality
 contracts on, 75, 78
 lack of, 14
 library privacy policies, 65
 of library records, 15
 library workers and, ix
 privacy audit for, 44
“consent,” 57
contract addendum, 78–79
contract negotiation, 75
contracts
 consistent process for, 78–79
 red flags in, 76
 vendor contracts, 75–76
conversation starters, 14–15
cookies
 in library privacy policy, 66
 in privacy policy, 55–56
 tracking pixels and, 59
core questions, 46–47, 50
Cornell University Library, 65
culture, organizational, 20
- D**
Dashlane password manager, 3
data
 See user data
data, ownership of, 59–60
“data broker,” 57
Data FOMO (fear of missing out), 36
data lifecycles
 data about user/data linked to user, 34

- data lifecycles (*continued*)
 - introduction to, 33
 - Library User Data Lifecycle, 34–41
- data security, 67
- deletion, data, 41
- democracy, 14
- digital security
 - digital security detective, 9–10
 - introduction to, 1
 - malware, 6
 - multi-factor authentication, 3–4
 - network privacy, 7–8
 - passphrases, 2
 - password managers, 3
 - passwords, creating strong/secure, 2
 - phishing, 4–5
 - ransomware, 6–7
 - staff/user training, 8
- digital security detective, 9–10
- disclosure of information, 59
- discussing users, 24–25
- documents
 - audit findings, 50
 - retention of, 28
 - user data storage, 36–37
- E**
- electronic access, 38–39
- electronic equipment, 41
- elevator speech, 15–16
- e-mail
 - clear GIFs, web beacons, tracking pixels, 58
 - malware from, 6
 - phishing, 4–5
 - ransomware from, 6
 - vendor policy on, 59
- empathy map
 - function of/example of, 12
 - in privacy exercise, 13–14
- encryption, 7–8
- equity, 15
- evaluation, of vendor privacy, 71–80
- evaluation questions, 73–74
- exercise
 - for access to user data, 38–39
 - for anonymizing holds, 29–30
 - for audience identification, 13–14
 - for contracting process, 78–79
 - for deletion of data, 41
 - Digital Security Detective, 9–10
 - for discussing users, 24–25
 - for library privacy advocacy, 18, 19
 - for Library User Data Lifecycle, 35–36
 - for multi-factor authentication, 4
 - for network privacy, 8
 - for overdue items, 26
 - for paper trail, 27–28
 - for passphrases, 2
 - for privacy audit framework, 45–47
 - for privacy audit guidelines/checklists, 48–49
- for privacy audit schedule, 51
- privacy policy scavenger hunt, 60–61
- for private spaces, 22–23
- for ransomware, 7
- for receipts, 3031
- for self-service discovery, 32
- for talking points, 15, 16
- for user data retention, 40
- user data storage scavenger hunt, 37
- for vendor contract red flags, 77
- for vendor contracts/licensing, 75–76
- for vendor privacy evaluation, 72, 74
- for vendor product/user privacy evaluation, 80–81
- for vendor selection process, 70–71
- for writing privacy policy, 61–63
- for writing your privacy policy, 64–68
- “explicit/informed consent,” 57
- external flash drives, 6
- F**
- Facebook, 58
- facial recognition software, 19, 68
- Family Educational Rights and Privacy Act, 39
- finances, 25
- fourth party
 - sharing user information with, 57–58
 - vendor privacy evaluation, 73
- free products, 80
- G**
- GIFs, 58–59
- Google
 - sharing of user data, 58
 - third-party integrations for user authentication, 58
 - “Transparency Report,” 68
- GPS coordinates, 58
- guidelines
 - for privacy audits, 48–49
 - for writing privacy policy, 61–62
- H**
- hard drives, 41
- headphones, 22
- Higher Education Community Vendor Assessment Toolkit, 79
- holds, anonymizing, 28–30
- HTML.com, 56
- HTTPS (Hypertext Transfer Protocol Secure), 7–8, 66
- I**
- indemnity/liability clauses, 76
- information security standards, 73
- “information we collect” phrase, 55
- Institute of Museum and Library Services (IMLS), ix
- intellectual freedom, 44
- ISO/IEC 27001 standard, 73
- IT department, 80
- K**
- K–12 Schools, 26
- L**
- labeling, 31
- LastPass, 3
- “Law Enforcement Inquiries: Key Concepts” (American Library Association), 39
- law enforcement requests
 - in library privacy policy, 68
 - policy for, 39
 - vendor disclosure of user data, 59
- legal regulations, 40
- Let’s Encrypt, 7, 66
- librarians
 - See library workers
- library
 - discussing users, 24–25
 - malware security for, 6
 - non-tech privacy, 21–32
 - overdue items, privacy and, 25–26
 - paper trail, following, 26–28
 - privacy audits, importance of, 44
 - privacy policy of, 53–54
 - privacy talking points, 14–15
 - private spaces, creating, 22–23
 - staff/user training for digital security, 8
 - user data collected by, 34
 - user surveillance in, 24
- Library Bill of Rights (American Library Association), 28–29
- library card applications, 28
- library documents
 - See documents
- Library Freedom Institute, 64
- library privacy advocacy
 - case studies, 19
 - relationships for, 20
 - ways to be advocate, 18
- Library User Data Lifecycle
 - access, 38–39
 - collection, 34–36
 - deletion, 41
 - diagram of, 35
 - reporting, 39
 - retention, 40
 - storage, 36–37
- library workers
 - accounts about digital security, 9–10
 - discussing users, 24–25
 - library privacy advocacy by, 18–19
 - privacy field guide for, ix–x
 - purchasing, control over, 70–71
 - staff/user training for digital security, 8
 - user privacy protection responsibility, 15
- licensing, 75–76
- links
 - malware and, 6
 - phishing scam, 5
 - in privacy policy, 65, 67
 - location data, 58

LTI (learning tools interoperability), 79

M

malware (malicious software), 6
Microsoft, 58
minors, 66
 See also children
mobile devices
 log-ins for, 37
 malware security for, 6
 physical access to, 38
multi-factor authentication (MFA)
 exercise for, 4
 overview of, 3
Multnomah County Library, Privacy and Confidentiality of Library Records, 65

N

network privacy, 7–8
network security, 67
NIST cybersecurity and privacy frameworks, 73–74
non-personal information, 55
non-tech privacy
 discussing users, 24–25
 holds, anonymizing, 28–30
 introduction to, 21
 overdue items, 25–26
 paper trail, following, 26–28
 private spaces, creating, 22–23
 receipts, 30–31
 self-service discovery, 31–32
 user surveillance, 24

O

1password, 3
online public access catalogs (OPACs), 31–32
operating system (OS)
 data about user's activities, 34
 non-personal information, 55
 updates for malware security, 6
"opt-in," 57
"opt-out," 57
organizational culture, 20
overdue items, 25–26
ownership of data, 59–60

P

paper documents
 paper trail, following, 26–28
 shredding, 41
paper scavenger hunt, 27–28
passphrases, 2–3
password managers, 3
passwords
 cookies and, 56
 creating strong/secure, 2
 for digital files, 38
 Digital Security Detective, 9
 password managers for, 3
 storage of user data, 37

PCI-DSS standard, 73
permanent cookies, 56
persistent cookies, 56
Personally Identifiable Information (PII)
 data about user/data linked to user, 34
 deletion of user data, 41
 examples of, 25
 in library receipts, 30–31
 overdue items and, 26
 paper trail, following, 26–28
 in privacy policy, 55
 privacy policy on collection of data, 65
 privacy protections for user data, 71
 reporting and, 39
 third-party integrations for user authentication and, 58
persuasive arguments, 17, 18
phishing, 4–5
phrases
 commonly used phrases/terms in privacy policy, 55–61
 vendor contract red flags, 76–77
physical access, 38–39
plain language tips, 62
Plain Language website, 61
Plain Writing Act, 61
policy
 for law enforcement requests, 39
 retention policy for user data, 40
 See also privacy policies
"Position Statement on Labeling Practices" (AASL), 31
"principle of least privilege," 38
priority 1 items, 48
priority 2 items, 48
priority 3 items, 48
privacy
 ALA privacy guidelines/checklists, 48
 data lifecycles, 33–41
 digital security, 1–10
 introduction to book, ix–x
 non-tech privacy, 21–32
 privacy audits, 43–51
 privacy policies, 53–68
 pushing for privacy in your organization, 80–81
 vendor audits, 79–80
 vendor privacy, evaluating, 71–80
 vendors and, 69–81
 See also user privacy
privacy, how to talk about
 audience, determination of, 12–14
 case studies, 19
 general talking points, 14–15
 introduction to, 11
 library privacy advocacy, 18
 organizational culture and, 20
 persuasive arguments, creating, 17
 privacy point, getting across, 15–16
"Privacy: An Interpretation of the Library Bill of Rights" (American Library Association), 57

Privacy and Confidentiality in the Cornell University Library, 65

privacy audits
 audit framework, building, 45–47
 definition of, 44
 guidelines/checklists for, 48–49
 importance of, 44
 introduction to, 43
 performing audit, 50
 repeating, 51
 telling audit story, 50–51
"Privacy Checklist Overview" (American Library Association), 49
"Privacy Field Guides" (IMLS & ALA), ix
privacy point, 15–16
privacy policies
 commonly used phrases/terms, 55–61
 definition of, 54
 how to write privacy policy, 61–63
 introduction to, 53
 reading, 54
 writing your privacy policy, 64–68
privacy protections, 71
privacy screens, 22
privacy statement, 64–65
Privacy Subcommittee of ALA's Office for Intellectual Freedom, ix
private spaces, 22–23
proctoring software, 19, 68
public computers, 66–67
public library
 library privacy advocacy scenario, 19
 overdue items and, 26
purchasing, 70–71

Q

questions
 for privacy audit, 45–47, 50
 for vendor privacy evaluation, 73–74
 for writing privacy policy, 62–63

R

ransomware, 6–7
reading
 commonly used phrases/terms in privacy policy, 55–61
 privacy policies, 54
receipts, 30–31
record retention schedule, 40
records, 41
 See also documents
red flags
 avoiding, 67
 contract addendum to address, 78
 in vendor contract, 76
 in vendors' privacy policies, 57–60
relationships, 20
reporting, 39
Request for Proposals (RFP), 72
resources
 on cookies, 56
 library privacy policies, 65

- resources (*continued*)
- for malware security, 6
 - privacy policy template, 64
 - for staff/user training in digital security, 8
- “Responding to Law Enforcement Inquiries: Suggested Guidelines” (American Library Association), 39
- retention
- of library documents, 28
 - in privacy policy, 65
 - of user data, 40
- RFP (Request for Proposals), 72
- Rutgers University Libraries, Privacy Policies, 65
- S**
- San José Public Library, Privacy Policy, 65
- Santa Cruz Public Library’s Vendor Security Assessment Questionnaire, 79
- Scavenger Hunt exercise
- for privacy policy, 60–61
 - for user data storage, 37
 - for vendor contract red flags, 77
- schedule
- privacy audit schedule, 51
 - record retention schedule, 40
 - for updates, 6
- school libraries
- library privacy advocacy, 19
 - privacy policy for, 54
 - self-service discovery, 31
 - user privacy protection, 39
- security
- in privacy policy, 60
 - standards, for vendor privacy evaluation, 73–74
 - of user’s PII, 28
 - See also* digital security
- security cameras
- in library privacy policy, 68
 - user surveillance in library, 24
- self-evaluation, 38
- self-service discovery, 31–32
- selling information, 57–58
- session cookies, 56
- sharing
- of audit story, 50–51
 - information in vendor privacy policy, 57–58
- shredding
- deletion of user data, 41
 - of library documents, 28
- software
- decision to buy, who controls, 70
 - malware, 6
 - proctoring software, 19
 - vendor audits, 79
 - vendor contract red flags, 76
 - vendor privacy protections, 71
- spreadsheet, 50
- SSL certificates, 7, 8
- staff, 8
- See also* library workers
- stakeholder, 13–14
- standards, 73–74
- storage
- in Library User Data Lifecycle, 36–37
 - of PII, 28
 - storing/tracking location data, 58
 - vendor storage of user data, 73
- storytelling
- in persuasive argument, 17
 - telling audit story, 50–51
- students
- privacy protection for, 66
 - self-service discovery, 31–32
- surveillance
- in library privacy policy, 68
 - privacy talking points, 14, 15
 - user surveillance in library, 24
- T**
- talking about users, 24–25
- talking points
- general, 14–15
 - getting privacy point across, 15–16
 - knowledge of audience and, 12
- tasks, of audit, 50
- temporary cookies, 56
- terms, 55–61
- testing
- of passphrase, 2
 - of privacy field guide, x
- third parties
- “third party” term in privacy policy, 56
 - third-party integrations for user authentication, 58
 - vendor contract red flags, 76
 - vendor contracts/licensing and, 75
- third-party vendors
- in library privacy policy, 67
 - vendor privacy evaluation, 73
- Tijerina, Bonnie, ix–x
- timeline, for privacy audit, 50
- TLS certificates, 7, 8
- tracking
- by cookies, 55–56
 - data brokers and, 57
 - location data, 58
 - pixels, 58–59
 - privacy audits and, 44
 - vendor contract red flags, 76
- training, 8
- “transparency report,” 68
- two-factor authentication
- See* multi-factor authentication
- U**
- updates, 6
- URL, 5
- user data
- audit framework, building, 45–47
 - data about user/data linked to user, 34
 - data lifecycles, 33
 - Library User Data Lifecycle, 34–41
 - ownership of, 59–60
 - privacy audits, function of, 44
 - privacy policy, phrases/terms of, 54–61
 - privacy policy, writing, 64–68
 - pushing for privacy in your organization, 80
- user permissions, 39
- user privacy
- holds, anonymizing, 28–30
 - how to protect, 39
 - Library User Data Lifecycle, 34–41
 - paper trail and, 26–28
 - privacy audits, function of, 44
 - vendors and, 69
- user surveillance, 24
- users
- authentication, third-party integrations for, 58
 - data about/data linked to, 34
 - discussing, 24–25
 - holds, anonymizing, 28–30
 - non-tech privacy, 21
 - overdue items and, 25–26
 - paper trail, user privacy and, 26–28
 - privacy policy and, 54, 55–61
 - private spaces for, 22–23
 - self-service discovery, 31–32
 - staff/user training for digital security, 8
- V**
- Vendor Contract and Privacy Rubric, 75
- vendor selection process
- exercise for, 70–71
 - shopping with privacy in mind, 71–72
- vendors
- access to user data, 39
 - audits of, 79–80
 - decision to buy, who controls, 70–71
 - evaluating vendor privacy, 71–80
 - in library privacy advocacy scenario, 19
 - privacy audits and, 44
 - privacy policies of, 54
 - privacy policy, phrases/terms of, 54–61
 - pushing for privacy in your organization, 80–81
 - user privacy and, 69–81
- W**
- web beacons, 58–59
- website
- clear GIFs, web beacons, tracking pixels, 58–59
 - HTTPS, moving library website to, 7–8
 - in library privacy policy, 66–67
 - user consent on, 57
 - See also* resources
- writing
- how to write privacy policy, 61–63
 - your privacy policy, 64–68