Chapter 5

Data Security, Integrity, and Retention

What data is collected and how libraries use such data—the topic of preceding chapters—is important. So, too, are the protections related to—and ultimate disposition of—data that is collected. This chapter focuses on data security and integrity and on the ultimate disposition of that data (data retention practices). To begin, the analyzed policies provide varying levels of detail regarding their libraries' data integrity and security practices. ALA's Privacy Tool Kit section "Developing or Revising a Library Privacy Policy" notes the following, and this verbiage appears in several of the library policies analyzed:

> **Data Integrity:** The library needs to assure data integrity. Whenever personally identifiable information (PII) is collected, the library must take reasonable steps to ensure integrity, including using only reputable sources of data, providing library users access to their personal data, updating information regularly, destroying untimely data or converting it to anonymous form, and stripping PII from aggregated, summary data. The library staff is responsible for destroying information in confidential or privacy-protected records to ensure against unauthorized disclosure. Information that should be regularly purged or shredded includes PII on library resource use, material circulation history, security/surveillance tapes, and both paper and electronic use logs.[1]

The ALA guidance also includes recommendations regarding data security (including administrative measures):

> **Security:** Security involves both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of data. Security measures should be integrated into the design, implementation, and day-to-day practices of the library's entire operating environment as part of its continuing commitment to risk management. This should include the guarantee of a secure wireless network for patrons to use. These measures are intended to prevent corruption of data, block unknown or unauthorized access to library systems and information, and provide reasonable protection of private information in a library's custody, even if stored offsite on servers or backup tapes.
>
> **Administrative Measures:** The library needs to implement internal organizational measures that limit access to data while ensuring that individuals with access do not utilize the data for unauthorized purposes. The library must also prevent unauthorized access by using technical security measures like encrypting transmitted and stored data, limiting access by using passwords, and storing data on secure servers or computers inaccessible by modem or network. If libraries store PII on servers or backup tapes offsite, they must ensure that comparable measures to limit PII access are followed. Libraries should also develop routine schedules for shredding PII collected on paper.[2]

Discussion of data integrity and security practices did not appear to be a major focus for many policies. Several library policies directly and honestly note the challenges of safeguarding data. Southern Illinois University Morris Library's policy notes, "Although no method can guarantee the complete security of data, we take steps to protect the privacy and accuracy of patron data."[3] The University of California San Diego Library's policy notes,

> To guard against unauthorized access, maintain data accuracy, and promote the correct use of information, we have implemented physical,

electronic, and managerial procedures to safeguard and secure the information we collect online.

However, while we consider these measures reasonable, no guarantee can be given that they will always prevent or protect against invalid access or improper activity. For this reason, we avoid keeping information beyond the term of its primary use and, where possible, encrypt or delete data elements that might cause activities to be linked to individual users.[4]

The University of Chicago Library's privacy policy notes, "While the Library makes a concerted effort to protect personal information, we cannot guarantee that your submissions to our website, any content residing on our servers, or any transmissions from our server will be completely secure."[5]

In a different light, an ancillary document to the University of California Berkeley Library's policy notes the possibility of unintentional observation of data:

> **Unavoidable Inspection.** During the performance of their duties, personnel who operate and support electronic communications resources periodically need to monitor transmissions or observe certain transactional information to ensure the proper functioning and security of Library systems and services. On these and other occasions, systems personnel might observe personally identifiable information. Except as provided elsewhere in this Policy or by law, they are not permitted to seek out such information where not germane to the foregoing purposes, or disclose or otherwise use what they have observed.[6]

Numerous public library policies (much more frequently than academic library policies) reference the challenging security associated with Wi-Fi networks. For example, the St. Louis Public Library's "Library Technology Acceptable Use Policy" notes,

> Users should be aware that the Internet is not a secure medium and that third parties may be able to obtain information regarding users' activities. . . .
>
> Users should understand and acknowledge that Hotspots are unsecured, wireless networks and that any information being sent or received over the network could potentially be intercepted by another wireless user. Users are cautioned against transmitting their credit card information, passwords, and any other sensitive, personal information while using the wireless network.[7]

Other policies note care should be taken with configuration of personal devices, such as Las Vegas–Clark County Library District's "Internet and Wireless Use Policy":

> **Use of Personal Equipment**
>
> . . .
>
> In light of security issues and the variety of equipment that can be used to access wireless networks, the District urges patrons to incorporate appropriate protections systems such as anti-virus, firewall software and updated patches when accessing the District's wireless network. The District does not provide encryption services and does not guarantee privacy of data transmitted across its network.[8]

Retention of Data

Often associated with the collection of data is the retention of data, as together they comprise the data life cycle. ALA's *Resolution on the Retention of Library Usage Records* notes,

> Dispose of library usage records containing personally identifiable information unless they are needed for the efficient and lawful operation of the library, including, but not limited to, data-related logs, digital records, vendor-collected data, and system backups. . . .
>
> The American Library Association urges members of the library community to advocate that records retention laws and regulations limit retention of library usage records containing personally identifiable information to the time needed for efficient operation of the library.[9]

The Privacy Tool Kit's section "Developing or Revising a Library Privacy Policy" notes,

> **Data Retention:** It is the responsibility of library staff to destroy information in confidential or privacy-protected records in order to safeguard data from unauthorized disclosure. Information that should be regularly purged or shredded includes PII on library resource use, material circulation history, and security/surveillance tapes and logs. If this data is maintained off-site, library administrators must ensure that appropriate data retention policies and procedures are employed.[10]

Some of the analyzed policies provided broad, generalized references to length of data retention, with phrasings such as "regularly remove," as opposed to

something more specific, such as "each week." Some policies provide additional, more detailed retention information on one or more particular data types. Examples of broad, generalized data retention references follow (and note some of the policies below provide more specific retention details later in their policies):

Indiana University Libraries

> In all cases involving personally identifiable information, it is our policy to . . . avoid retaining records not needed for the fulfillment of the mission of the library.
>
> . . .
>
> Our goal is to collect and retain only the information we need to provide library-related services.
>
> . . .
>
> *Data Integrity:* We take reasonable steps to assure data integrity, including . . . destroying untimely data or converting it to anonymous form.
>
> *Data Retention:* We regularly review and purge personally identifiable information once it is no longer needed to manage library services. Information that is regularly reviewed for purging includes, but is not limited to, personally identifiable information on library resource use, material circulation history, and security/surveillance tapes and logs.
>
> . . .
>
> The IU Libraries follow University policy for the retention of data. . . .
>
> Data about which users were connected to which machine is collected, in accordance with University policy, and kept for a limited time with very limited access by staff.
>
> . . .
>
> We regularly remove cookies, web history, cached files, and other use records from library computers and networks.[11]

University of Michigan Library

> **How long will you keep data about the use of Library services?**
>
> It depends on the data and how we are using it. Some data will be kept indefinitely, other data is stored and used for shorter periods. We only keep data as long as it is useful for the services we provide.[12]

University of Chicago Library

> Identifiable information may be retained, in some cases indefinitely, when doing so serves an institutional purpose.[13]

University of California San Diego Library

> Where it is necessary for the Library to identify users, it is our goal to gather only the minimum information necessary and to retain that information for only as long as it is needed to complete a particular transaction.
>
> . . .
>
> **Site Security**
>
> We avoid keeping information beyond the term of its primary use and, where possible, encrypt or delete data elements that might cause activities to be linked to individual users.[14]

Mount Prospect Public Library

> The Library will make all practicable efforts to retain records containing patron-identifiable information only to the extent necessary to preserve Library or public property or to fulfill another core library function.[15]

Pierce County Library System

> Library records containing personally identifiable information will be disposed of unless needed for efficient operation of the library, public records retention requirements, system backups, or other reasons related to effectively managing library resources or providing services.[16]

Las Vegas–Clark County Library District

> In accordance with NRS 239, the District will not retain any records pertaining to a patron's use of library resources longer than necessary to provide appropriate stewardship of those resources.
>
> . . .
>
> *Data Retention:* The District protects personally identifiable information from unauthorized disclosure once it is no longer needed to manage library services. Information that should be regularly

> purged or shredded includes personally identifiable information on library resource use, material circulation history, and security/surveillance tapes and logs.[17]

ALA's "Library Privacy Checklist—Overview" (as well as the checklists associated with specific systems) provides additional retention guidance on particular data types, for example, circulation transaction data: "Purge circulation and interlibrary loan records when they are no longer needed for library operations. Any patron data that is kept for analysis should be anonymized or de-identified and have access restricted to authorized staff."[18]

Indeed, across the analyzed policies, one of the most frequent retention-related references to a specific data type is circulation data. In many but not all instances, it's noted that upon the return of an item to the library, the information tying the patron to that item is erased. Many policies note exceptions related to instances in which a fine or fee is accrued or in which a user has opted for the system to maintain a list of past items checked out. Library policies can provide more time frame–specific information on one or more data types, such as

- circulation data
- interlibrary loan and document delivery data
- end user computer and resource use data
- reference transaction data
- video surveillance data
- patron record data
- social media and shared content data
- various types of computer use and network-related data, whether on a client or server computer

Circulation Data

Cornell University Library

> The Library seeks to protect user privacy by purging borrowing records as soon as possible. In general, the link connecting a patron with a borrowed item is broken once the item is returned. The exception is when a bill for the item is generated. In that case, the information on who borrowed the item is retained indefinitely in our system.[19]

Utah State University Libraries

> To safeguard patron information once a book is returned to the library the link between a patron and the item checked out is deleted. The only exception to this deletion is for books with fines or those books regarded as "lost" on a patron's account.[20]

University of Utah J. Willard Marriot Library

> The Library purges from its system all circulation records 30 days after a circulation transaction has closed and the items have been returned.[21]

University of Texas Libraries

> When a borrower returns materials to the library, if no fines or fees are assessed, information about the materials checked out is deleted from the library's online records twice monthly.[22]

Temple University Libraries

> The records of most circulation borrowing transactions are expunged and overwritten immediately upon return to the libraries of the loaned items and thereafter are reflected only as anonymized statistics descriptive of overall borrowing patterns.[23]

Southern Illinois University Morris Library

> Morris Library maintains records of circulation transactions only until the borrowed items are returned. Fines accrued for lost or overdue books are kept for record keeping purposes and only until the patron's record is purged. The library does not maintain histories of patrons' previously borrowed items.[24]

San Diego State University Library

> The Library will not track identifiable patron search history and will keep no record of such. The exceptions to this are:
>
> 1. In circumstances where format of material requires extensive time to verify the return of all relevant borrowed items (ie: a box containing dozens of documents etc). After full verification the patron data will not be kept except in the cases of rare and valuable materials where usage data may be kept indefinitely.[25]

University of Denver Libraries

> WHEN YOU CHECK OUT PRINT MATERIALS:
>
> . . .
>
> Once you return an item, and you do not owe a fine on the item, your checkout of the item is anonymized and the item cannot be traced back to you.[26]

East Greenbush Community Library

> Items that have been returned are automatically erased from a patron's record, unless they have opted to save their checkout history.[27]

Fairbanks North Star Borough Public Libraries

> The library does not maintain records of items that individuals have borrowed and returned in the past, except when there are unresolved issues with those items.[28]

Geauga County Public Library

> Circulation records and other records identifying the names of library users with specific materials are retained while the materials are charged to a patron and when materials are returned until of no further administrative value. The current ILS system retains patron information on items until the item is checked out to another patron.
>
> If an item is returned damaged and the fees are not paid, the library will retain the record until the matter is resolved.[29]

Queens Borough Public Library

> At the moment that library material is returned to the library, the link between the customer and the material is broken—the Library's system does not retain information on what materials were taken out by whom the moment the item is returned.[30]

Brown County Library

> The Library does not maintain a history of what a library user has previously checked out once books and materials have been returned on time. When fines accrue on a user's account, the Library does maintain records of items that have been borrowed but returned after the due date, or are still outstanding on the user's record.[31]

Jessamine County Public Library

> Personal data is privatized, i.e. made anonymous, in the Library's computer system so that log files cannot identify personal checkout history beyond 60 days.[32]

Las Vegas–Clark County Public Library

> District records that link a patron's identity to the use of library materials will be expunged upon the return in good standing of loaned materials to the District.[33]

San José Public Library

> The library does not keep a record of your reading history beyond operational requirements. Once you return an item it is removed from your account.[34]

Interlibrary Loan and Document Delivery Data

San Diego State University Library

> Information on materials received through Interlibrary Loan (ILL) are [*sic*] kept for one year.[35]

Berkshire Athenaeum

> The Athenaeum tracks interlibrary loaned items currently being borrowed and generates a paper record with patron information. After a period of six months, once the materials are returned to the owning library and all appropriate fines and/or fees are paid by the borrower, the paper trail record is destroyed.[36]

End User Computer and Resource Use Data

Cornell University Library

> Raw log files are normally maintained for 90 days for security purposes. . . . For some sites, an aggregated abstract of the data is prepared each night that anonymizes session data so that searches cannot be linked to specific IP addresses or network IDs.[37]

Harvard Library

> Data gathered about each session varies according to the method of connection to the resource. The resulting logs contain information necessary for analyzing the use of resources, troubleshooting problems and improving services.
>
> Log data is also used to distribute resource costs among Harvard libraries and faculties. These logs remain intact for approximately one fiscal year.[38]

University of Texas Libraries

> The University of Texas Libraries keeps the minimum number of records necessary to maintain operations. For example, when a user logs off a library computer, the library does not retain information that connects the user to activities performed during the session.[39]

University at Albany Libraries

> **Retention of Information Collected through This Web Site**
>
> In general, the Internet services logs of the University Libraries, comprising electronic files or automated logs created to monitor access and use of Agency services provided through this Web site, are retained for 60 business days and then destroyed. Occasionally, logs are retained longer for troubleshooting purposes. Information concerning these records retention and disposition schedules may be obtained through the Internet privacy policy contact listed in this policy.[40]

Southern Illinois University Morris Library

> Cookies, web history, and cached files are removed when a user closes a browser or logs off a machine.[41]

Rutgers University Libraries

> We remove cookies, web history, cached files, or other computer and Internet use records and other software code that is placed on our public computers or networks after each use.[42]

Warrenville Public Library District

> Public Access Computers
>
> The Warrenville Public Library District attempts to maintain strict security on public access computers to prevent any personal information from being retained after a workstation has been rebooted.[43]

Berkshire Athenaeum

> Once a search has been conducted, the software does not retain a copy of the search, and any records of the search will not exist.
>
> . . .
>
> The reservation management program retains patron identification information for only the current day's transactions. After the end of the business day, session information and statistical summary information can be generated; but patron identifying information is unavailable.
>
> Printouts from the library's public internet workstations are managed with an automated print management program. The program confirms print requests and alerts patrons and staff of print charges accrued. After a pending print job is released by staff for print out no record of the job remains.
>
> The security on the workstations wipes out the cache and/or history files each time a new computer session is started.
>
> . . .
>
> The search history of each PAC [catalog only station] is automatically erased every twenty-four hours.[44]

Ocean County Library

> When a computer session is ended, all information about that session is ordinarily deleted. At the end of the business day, all computer use and reservation records are normally erased.[45]

Durham County Library

> To use one of our public computers, you log on using your library card number. We do not keep a record of your activities during your session, such as browsing history, cookies, bookmarks, or downloads. The session data is automatically deleted from the computer after you log out. We do, however, keep a record of the fact that you logged on to that computer.[46]

Tampa-Hillsborough Public Library

> In accordance with this law [Florida Statutes Chapter 257.261], computer sign-in sheets are shredded as soon as all customers listed have been served or at the end of the day, whichever occurs first.
>
> . . .
>
> A library branch may choose to keep a daily log of guest pass distribution. . . . Sign-in sheets are to be shredded as soon as they are full or at the end of each day, whichever occurs first.[47]

San José Public Library

> The library does not keep a record of your activities on any public computer or laptop. Any record of browsing history and activities are [*sic*] removed when you log out.
>
> All personally identifiable information is purged immediately upon the end of your public computer reservation. An anonymous log is created that

includes only the computer terminal number, reservation time, and duration of the session. These anonymous reservation statistics remain in the system for two months.

All connected devices you borrow from the library (e.g. tablets, eReaders) have their history manually cleared by library staff immediately after you return the device.[48]

Reference Transaction Data

Texas State University Libraries

User Privacy

- The Alkek Library Ask a Librarian service records all reference transactions, including the chat conversation and the URLs for all the web sites visited.
- At the end of the session, you have the option to have the transcript emailed to you and a copy will be stored in our database for a period of one year.[49]

Temple University Libraries

Any patron may request to have their chat, email, or text transcript deleted by contacting the Libraries' Learning and Research Services department.[50]

Southern Illinois University Morris Library

In the case of email reference questions, we retain any personal information provided by the patron, such as name, email, phone number, until the question is resolved.[51]

Brown County Library

The Library treats reference questions, regardless of format of transmission (in person, via telephone, fax, email or online) confidentially. Identifying information related to these questions is purged on a minimum of two weeks.[52]

Video Surveillance Data

Berkshire Athenaeum

Video Surveillance: . . . Recorded images are saved for a period of eight weeks, at which point the storage medium is re-recorded.[53]

Western Plains Library System

Recordings from the WPLS video security system are stored digitally on restricted hardware at the Main Office and retained up to a minimum of 28 days. . . . Video records of incidents can be retained and reviewed as long as considered necessary by the Executive Director.[54]

Deer Park Public Library

Length of time recorded images are retained varies based on the storage capacity of the system hard drive.[55]

Mount Prospect Public Library

No video will be stored for more than the rolling window when the system overwrites the oldest video while recording the present.

. . .

The Library will retain specific footage of an incident until no longer needed. Video files will be reviewed annually by the Executive Director and the Director of Facilities and Security to decide whether to continue to retain or to dispose.[56]

Ocean County Library

Recorded information from security cameras is retained for one month, unless an incident occurs that requires holding the tape longer. . . .

Recorded information that is subpoenaed will be retained for one year.[57]

Las Vegas–Clark County Library District

Recordings from security cameras are stored no longer than 10 days, unless an incident occurs that requires holding the entire recording or a portion of the recording longer.[58]

Patron Record Data

Jessamine County Public Library

When a customer record is inactive for four (4) years and carries no outstanding debt (financial or in borrowed materials), the record is deleted from the Library's computer system and is not archived.[59]

Brown County Library

> **Library Cards and Circulation Records**
>
> To receive a library card, library users are required to provide identifying information such as name, birth date and mailing address. This identifying information is retained as long as the library user continues to use the library card.[60]

Pinellas Public Library Cooperative

> Cardholder accounts will be purged after 5 years of inactivity unless there are billed item fees on the account. All accounts, including delinquent accounts with billed item or collection referral fees, will be purged after 7 years of inactivity. Libraries follow the Florida Department of State's *General Records Schedule for Public Libraries* when reviewing records eligible for purging.[61]

Durham County Library

> For most cardholders, your account remains in the system as long as it is active. An account becomes inactive when it hasn't been used in three years and there are no outstanding fines or fees attached. At that point, it is deleted from our system. A few card types, such as non-resident cards, expire sooner—see our Registration Policy for details.[62]

Social Media and Shared Content Data

Nashville Public Library

> **The Library Is Bound by Records Retention Rules**
>
> What this means: A record of your usage and content will likely exist.
>
> All designated Metro government social media accounts shall follow archive guidelines set forth by the Public Records Commission.[63]

St. Louis Public Library

> Think before you post. You are legally liable for everything you post. Remember that the internet never forgets. Everything you post may be visible to the world even after you attempt to delete it.
>
> The content of the Library's social media is subject to public record laws, including the Missouri Sunshine laws. Relevant record retention schedules apply to social media content. Content must be managed, stored, and retrieved to comply with open records laws and e-discovery laws and policies.[64]

Hillsborough County Public Library Cooperative

> Moderators will maintain an archive containing all social media posts and comments in accordance with the State of Florida's General Records Schedule GS15 for Public Libraries.[65]

Parent Institution or System-wide Retention Schedules

Several library policies make reference to—and in some cases provide a link for—a different, higher-level record retention schedule or policy, such as a university schedule or a county government schedule.

University of Connecticut Library

> Library patron records are retained in accordance with the state record retention requirements established by the Office of the Public Records Administrator of the Connecticut State Library.[66]

University of California San Diego Library

> The Library's Billing Department retains all paper and electronic documents pertaining to and relevant for the collection of overdue fines, replacement charges, damaged-book fines/charges, and associated processing fees, according to the University of California Records Disposition Schedules Manual.[67]

Syracuse University Libraries

> The Libraries retain Individual Information associated with Business Transactions for a period of time mandated by state or federal tax laws, and consistent with the University's data retention schedule.[68]

Temple University Libraries

> At all times PII is to be secured in accordance with University policies and for limited time periods defined by record retention schedules.
>
> . . .
>
> Records containing PII which are scheduled for destruction shall be disposed of in accordance with University information security procedures.[69]

Cherokee Regional Library System

> The Cherokee Regional Library System shall follow the Local Government Records Retention Schedules for Local Government Paper and Electronic Records as set forth by the Georgia Secretary of State's Division of Archives and History.[70]

Genesee District Library

> **Records Retention**
>
> In order to meet the administrative, legal, fiscal, and archival requirements of the State of Michigan, the Genesee District Library will manage its records in accordance with the General Schedule #17 (GS #17) developed for Michigan public libraries.[71]

San José Public Library

> The library strives to collect the least amount of personally identifiable information we can. We avoid creating unnecessary records. We keep your information as long as required by the City of San José's Records Retention Schedule.[72]

Notes

1. American Library Association, "Developing or Revising a Library Privacy Policy," Privacy Tool Kit, last updated April 2017, www.ala.org/advocacy/privacy/toolkit/policy.
2. American Library Association, "Developing or Revising."
3. Southern Illinois University Morris Library, "Patron Privacy Policy," December 2, 2015, https://lib.siu.edu/about/policies/patron-privacy-policy.php.
4. University of California San Diego Library, "Privacy Policy," last updated August 24, 2004, https://library.ucsd.edu/about/policies/privacy-policy.html.
5. University of Chicago Library, "Privacy Statement," https://www.lib.uchicago.edu/about/thelibrary/policies/privacy/.
6. University of California Berkeley Library, "Collection, Use, and Disclosure of Electronic Information," last updated September 22, 2008, https://www.lib.berkeley.edu/about/privacy-electronic-information.
7. St. Louis Public Library, "Library Technology Acceptable Use Policy," last updated February 8, 2018, https://www.slpl.org/service-policies/technology/.
8. Las Vegas–Clark County Library District, "Internet and Wireless Use Policy," https://lvccld.org/wp-content/uploads/sites/54/2017/11/internet_wireless_use_policy.pdf.
9. American Library Association, *Resolution on the Retention of Library Usage Records* (Chicago: American Library Association, 2006), https://alair.ala.org/bitstream/handle/11213/1594/52.4.4%20Retention%20of%20Library%20Records.pdf.
10. American Library Association, "Developing or Revising."
11. Indiana University Libraries, "Indiana University Libraries Privacy Policy," last updated February 1, 2012, https://policies.iu.edu/policies/lib-01-libraries-privacy/index.html.
12. University of Michigan Library, "Library Privacy Statement—Frequently Asked Questions (FAQ)," last updated June 14, 2018, https://www.lib.umich.edu/library-administration/library-privacy-statement-frequently-asked-questions-faq.
13. University of Chicago Library, "Privacy Statement."
14. University of California San Diego Library, "Privacy Policy."
15. Mount Prospect Public Library, "Record Keeping Policy," https://mppl.org/wp-content/uploads/2018/07/Record-Keeping-Policy-0718.pdf.
16. Pierce County Library System, "Confidentiality of Library Records and Customer Files," last updated October 15, 2013, https://www.piercecountylibrary.org/about-us/policies/confidentiality-library-records.htm.
17. Las Vegas–Clark County Library District, "Patron Privacy Policy," last updated April 10, 2014, https://lvccld.org/wp-content/uploads/sites/54/2017/10/privacypolicy.pdf.
18. American Library Association, "Library Privacy Checklist—Overview," last updated January 26, 2020, www.ala.org/advocacy/privacy/checklists/overview.
19. Cornell University Library, "Library Practices on the Collection, Use, Disclosure, Maintenance and Protection of Personally-Identifiable Information," https://www.library.cornell.edu/practices.
20. Utah State University Libraries, "Utah State University Libraries Privacy Statement," https://arwen.lib.usu.edu/privacy_policy/.
21. University of Utah, J. Willard Marriott Library, "Privacy Policy," https://lib.utah.edu/pdf/Privacy_Policy_Procedures.pdf.
22. University of Texas Libraries, "Privacy and Confidentiality of Library Records Policy," https://www.lib.utexas.edu/about/policies/privacy-and-confidentiality-library-records-policy.
23. Temple University Libraries, "Confidentiality of Patron Records," last updated January 31, 2017, https://library.temple.edu/policies/confidentiality-of-patron-records.
24. Southern Illinois University Morris Library, "Patron Privacy Policy."
25. San Diego State University Library, "Freedom of Access and Privacy," https://library.sdsu.edu/about-us/policies-guidelines/freedom-access-privacy.
26. University of Denver Libraries, "Your Privacy and University Libraries," https://library.du.edu/policies/records-privacy.html.
27. East Greenbush Community Library, "Privacy Policy," https://eglibrary.org/about/policies/#privacy.
28. Fairbanks North Star Borough Public Libraries, "Borrowing Services," Policies and Procedures, last updated November 21, 2018, https://fnsblibrary.org/about/polpro/.
29. Geauga County Public Library, "Retention of Circulation Records," Geauga County Public Library Operating Policy Manual, December 17, 2019, http://divi.geaugalibrary.net/wp-content/uploads/2020/01/712-Retention-of-Records.pdf.

30. Queens Borough Public Library, "Privacy Policy," December 2003, https://www.queenslibrary.org/about-us/library-policies/privacy.
31. Brown County Library, "Privacy and Confidentiality," May 15, 2014, https://www.browncountylibrary.org/wp-content/uploads/2012/09/H_1-Privacy-and-Confidentiality.pdf.
32. Jessamine County Public Library, "Information Security Policy," last updated August 21, 2019, https://jesspublib.org/wp-content/uploads/3.6-Information-Security-Policy-2019-09-25.pdf.
33. Las Vegas–Clark County Library District, "Patron Privacy Policy."
34. San José Public Library, "Privacy Policy," last updated March 12, 2018, https://www.sjpl.org/privacy-policy.
35. San Diego State University Library, "Freedom of Access and Privacy."
36. Berkshire Athenaeum, "Guidelines for Confidentiality While Cooperating with Law Enforcement," 2010, https://static1.squarespace.com/static/5c7eed16e8ba44443d295e02/t/5cb177cdeb39315a7ce00238/1555134414545/BA_LawEnforcement_Confidentiality.pdf.
37. Cornell University Library, "Library Practices."
38. Harvard Library, "Harvard Library's Privacy Statement," Privacy, Terms of Use and Copyright Information, https://library.harvard.edu/privacy-terms-use-copyright-information#privacy.
39. University of Texas Libraries, "Privacy and Confidentiality."
40. University at Albany Libraries, "Internet Privacy Policy," https://library.albany.edu/privacy.
41. Southern Illinois University Morris Library, "Patron Privacy Policy."
42. Rutgers University Libraries, "Privacy Policy," October 19, 2010, https://www.libraries.rutgers.edu/privacy_policy.
43. Warrenville Public Library District, "Confidentiality of Library Records," Policy No. 420, www.warrenville.com/about/Policies/420ConfidentialityofLibraryRecords.pdf.
44. Berkshire Athenaeum, "Guidelines for Confidentiality."
45. Ocean County Library, "Computer Use and Internet Policy," last updated June 17, 2014, http://theoceancountylibrary.org/sites/default/files/internet%20policy.pdf.
46. Durham County Library, "Privacy Policy," July 2019, https://durhamcountylibrary.org/about/policies/privacy-policy/.
47. Tampa-Hillsborough Public Library, "Access to Electronic Resources," Policy No. LS 306, June 2018, https://www.hcplc.org/thpl/policies/300/LS306-Access-to-Electronic-Resources.pdf.
48. San José Public Library, "Privacy Policy."
49. Texas State University Libraries, "Virtual Reference Policy (Ask a Librarian @Alkek)," https://www.library.txstate.edu/about/policies/virtual-reference.html.
50. Temple University Libraries, "Virtual Reference Privacy Guidelines," https://library.temple.edu/services/privacy.
51. Southern Illinois University Morris Library, "Patron Privacy Policy."
52. Brown County Library, "Privacy and Confidentiality."
53. Berkshire Athenaeum, "Guidelines for Confidentiality."
54. Western Plains Library System, "Video Surveillance Policy," July 13, 2018, http://wplibs.com/wp-content/uploads/2018/10/Video-Surveillance-Policy.pdf.
55. Deer Park Public Library, "Security Camera Policy," last updated October 24, 2018, https://deerparklibrary.org/wp-content/uploads/2018/10/Security-Camera-Policy-Revised-Oct-24-2018.pdf.
56. Mount Prospect Public Library, "Video Surveillance Policy," 2019, https://mppl.org/wp-content/uploads/2019/05/Video-Surveillance-Policy-052919.pdf.
57. Ocean County Library, "Camera Surveillance," Policies, Fees and Forms, last updated April 19, 2016, https://theoceancountylibrary.org/policies-fees-forms.
58. Las Vegas–Clark County Library District, "Patron Privacy Policy."
59. Jessamine County Public Library, "Information Security Policy."
60. Brown County Library, "Privacy and Confidentiality."
61. Pinellas Public Library Cooperative, "Public Services Policies," May 31, 2019, www.pplc.us/misc-pdf/CirculationPolicy_2019.pdf.
62. Durham County Library, "Privacy Policy."
63. Nashville Public Library, "Social Media and Blog Guidelines for Using, Commenting, and More," https://library.nashville.org/about/policies/social-media-and-blog-guidelines.
64. St. Louis Public Library, "Social Media Guidelines," last updated April 3, 2017, https://www.slpl.org/service-policies/social-media-policy/.
65. Hillsborough County Public Library Cooperative, "Social Media Guidelines," Policy Number LS 1108, August 2018, https://www.hcplc.org/thpl/policies/1100/LS1108-Social-Media-Guidelines.pdf.
66. University of Connecticut Library, "Policy on Confidentiality of Library Client Records," https://lib.uconn.edu/about/policies/policy-on-confidentiality-of-library-client-records/.
67. University of California San Diego Library, "Privacy Policy."
68. Syracuse University Libraries, "Privacy Policy," version 2.0, last updated October 4, 2013, https://library.syr.edu/policy/documents/privacy-policy.pdf.
69. Temple University Libraries, "Confidentiality of Patron Records."
70. Cherokee Regional Library System, "Records Retention Policy," July 30, 2015, https://www.chrl.org/wp-content/uploads/2015/04/Records-Retention-Policy_Approved-July-30-2015.pdf.
71. Genesee District Library, "GDL Policy 6.9: Records Retention," *Policy Manual* (Flint, MI: Genesee District Library, 2016), https://www.thegdl.org/wp-content/uploads/Policies/Policy-Manual-for-Website.pdf.
72. San José Public Library, "Privacy Policy."