Operationalizing Library Privacy: Policies, Procedures, and Practice

Becky Yoose
Library Data Privacy Consultant, LDH Consulting Services
Pacific Library Partnership, February 2020

Pacific Library Partnership

This project was supported in whole or in part by the U.S. Institute of Museum and Library Services under the provisions of the Library Services and Technology Act, administered in California by the State Librarian. The opinions expressed herein do not necessarily reflect the position or policy of the U.S. Institute of Museum and Library Services or the California State Library, and no official endorsement by the U.S. Institute of Museum and Library Services or the California State Library should be inferred.

Workshop Housekeeping – Guidelines

- All responses and questions are valid.
- Assume good intent.
- When you disagree, challenge or criticize the idea, not the person.
- Be mindful of the time.
- One speaker at a time.
- Speak from your own perspective.
- Help protect others' privacy by observing the Chatham House Rule.

Workshop Housekeeping - Logistics

IANAL; Consult legal staff for legal advice

Exercises and Discussions - what to expect

Local practices vs vendor practices

Toolkit tie-in

Privacy measures are only as strong as the least-knowledgeable person working with patron data

Workshop Schedule

9:00 – 9:20: Welcome and housekeeping

9:20 – 10:00: Training and exercises

10:00 – 10:10: Break #1

10:10 – 11:15: Training and exercises

11:15 – 11:25: Break #2

11:25 – 12:15: Training and exercises

12:15 – 12:30: Wrap up

Introduce Yourself!

1. Name
2. Job title and where you work
3. What was the most recent data breach that included your personal data?

Have I Been Pwned?

https://haveibeenpwned.com/

Section One:
Setting the Groundwork

Terminology – Policy, Procedure, Practice

Policy

- High level statement set by organization
- Framework (or parameters) for which organization should operate in
- Provides guidance for operational goals and priorities
- Governs compliance with other policies, regulations, standards, etc.

Procedure

- Provides staff a process to implement policy
- Focus on specific areas of organization
- Gets to the “how, when, where, and who” of policy implementation

Practice

- Implementation of policy and procedure (P&P) in daily operations
- P&P subject to interpretation by staff based on current situation
- “What happens when you try to follow P&P at work” (AKA Reality)

Local **practice** is informed by **procedure**, **procedure** is informed by **policy**, **policy** is informed by ___

Ethics

Standards

Regulations

Best Practices

Privacy Operations - Stakeholders

- Library administrators
- Legal counsel
- Library board
- Parent organization/institution
- Library staff
- Patrons
- Community partners
- Professional organizations
- State libraries
- Vendors

Image source – Women In Tech - 65 by WOCinTech Chat, CC BY 2.0, https://www.flickr.com/photos/wocintechchat/22344392878/

Effective privacy operations…

Empower staff

Protect patrons

Minimize potential legal & financial liability

Exercise – Policy, Procedure, Practice… and PB&J

Where did **the public** factor into your conversations?

Section Two: Policies

Privacy Policies – Internal and External

Privacy Policy

- Communications to internal audiences
- Privacy policies can include:
  - Data collection, storage, retention, processing
  - Data security and privacy
  - Retention periods
  - Incident response (ex. data breach)
  - Sharing data with other departments and external third parties

Privacy Notice

- Communications to external audiences
- Privacy notices should:
  - Be accessible in both online and in physical formats
  - Explain privacy policies and user rights in simple, concise language to a general audience
  - Inform the reader of any policy changes

Both should go through legal review before final approval

What Privacy Policies to Have?

Minimum – Privacy and Confidentiality of Library Patron Data/Records

- Notice and consent
- Access to data by patrons
  - Special considerations for minors and authorized users
- Data disclosure to third parties
- Data collection, storage, and retention
- Data privacy and security
- Policy enforcement
- Policy audit and review
- State and local regulations compliance
- FERPA and COPPA considerations
- Law Enforcement Requests and other patron data request
  - Types of requests from law enforcement, including **judicial vs administrative warrants**

What Other Privacy-Related Policies to Have?

- BYOD (Bring Your Own Device)
- Social media
- Employee monitoring
- Access to patron data
- Telecommuting/Remote Work
- Data classification
- Handling/collecting personal data from minors
- Data collection for programs, events, community surveys, events, etc.
- Web analytics and tracking, including cookies and web beacons
- Incident response
- Privacy reviews and audits
- Other information security policies

Privacy Policies and Legal Regulations

Federal Regulations

- Bill of Rights Amendments (particularly the 4th)
- USA Freedom Act
- FERPA
- COPPA

Local Regulations

- County/City record retention schedules
- Public disclosure regulations
- Parent organization policies
  - Not a legal regulation, but still important to harmonize policies with overall organizational policies

Privacy Policies and Legal Regulations – California Gov Code § 6254

Disclosure exemption for:

> "(j) Library circulation records kept for the purpose of identifying the borrower of items available in libraries, and library and museum materials made or acquired and presented solely for reference or exhibition purposes. The exemption in this subdivision shall not apply to records of fines imposed on the borrowers."

Privacy Policies and Legal Regulations – California Gov Code § 6267

All patron use records of any library which is in whole or in part supported by public funds shall remain confidential and **shall not be disclosed by a public agency, or private actor that maintains or stores patron use records on behalf of a public agency, to any person, local agency, or state agency** except as follows:

(a) By a person acting within the scope of his or her duties within the administration of the library.

(b) By a person authorized, in writing, by the individual to whom the records pertain, to inspect the records.

(c) By order of the appropriate superior court.

Privacy Policies and Legal Regulations – California Gov Code § 6267 (con't)

As used in this section, the term "patron use records" includes the following:

(1) Any **written or electronic record**, that is **used to identify the patron**, including, but not limited to, a patron's name, address, telephone number, or e-mail address, that a library patron provides in order to become eligible to borrow or use books and other materials.

(2) Any **written record or electronic transaction** that **identifies a patron's borrowing information or use of library information resources**, including, but not limited to, database search records, borrowing records, class records, and any other personally identifiable uses of library resources information requests, or inquiries.

This section shall not apply to statistical reports of patron use nor to records of fines collected by the library.

Personally Identifiable Information [PII] and Library Patron Data

PII 1 - Data about a patron

- Name
- Physical/email address
- Phone number
- Date of birth
- Patron record number
- Library barcode

PII 2 - Activity that can be tied back to a patron

- Search & circulation histories
- Computer/wifi sessions
- Reference questions
- Electronic resource access
- IP Address
- Program attendance

What about… (Gray Areas)

Security camera recordings?

Library security incident reports?

Shift logs?

Staff email?

Other? Future technology? New services/programs?

Privacy Policies and Legal Regulations – California Consumer Privacy Act of 2018 (CCPA)

Regulates the sale (and to a lesser extent collection and processing) of personal information by covered businesses

Gives California residents:

- Right to access what personal information is collected and shared with service providers and other third parties
- Right to request deletion of personal information
- Right to opt out of sale of personal information

Areas of concern for libraries:

Household information

- Part of personal information definition
- Included as part of the response to access and deletion requests

13-16 year old affirmative consent

- Businesses must obtain affirmative consent from 13-16 year old users to sell personal information
- Possibilities:
  - COPPA liability
  - "Age-gating" sites and services – asking for age of users

Breather

Privacy Policies and Ethics, Standards, and Guidance

ALA

- Library Bill of Rights
- Privacy: An Interpretation of the Library Bill of Rights
- Code of Ethics
- Policy concerning Confidentiality of Personally Identifiable Information about Library Users
- Library Privacy Guidelines and Checklists
- **Video and electronic surveillance technologies guidance**
- **Law enforcement request guidance**

IFLA

- IFLA Statement on Privacy in the Library Environment
- IFLA Code of Ethics for Librarians and other Information Workers

CLA and California State Library

- Statements and recommendations (example – LinkedIn statement by both organizations)

Privacy Policies and Ethics, Standards, and Guidance

Fair Information Practice Principles

- Notice/Awareness
- Choice/Consent
- Access/Participation
- Integrity/Security
- Enforcement/Redress

OECD Privacy Principles

- Collection Limitation Principle
- Data Quality Principle
- Purpose Specification Principle
- Use Limitation Principle
- Security Safeguards Principle
- Openness Principle
- Individual Participation Principle
- Accountability Principle

Privacy Policies and Industry Best Practices

- Data minimalization
  - Limiting the collection of personal data to only what is required to meet a specific business need.
  - Current needs vs Data FOMO
- Principle of Least Privilege
  - Users, programs, etc. can only access the data necessary for performing intended function or duty.
- Information security practices
  - Data integrity and protection standards for data at rest and data in transit

Privacy by Design (PbD)

1. Proactive not reactive; preventive not remedial
2. Privacy as the default setting
3. Privacy embedded into design
4. Full functionality – positive-sum, not zero-sum
5. End-to-end security – full lifecycle protection
6. Visibility and transparency – keep it open
7. Respect for user privacy – keep it user-centric

Image source – Privacy by Rob Pongsajapan, CC BY 2.0, https://www.flickr.com/photos/pong/2404940312/

Building a Privacy Notice - Elements

- What user data is collected, processed, and retained
- How user data is collected
- Business reasons for collection and processing of user data
- What data is shared with third parties
- Business reasons for sharing user data with third parties
- How users can control collection of data
- How users can control sharing of data with third parties
- How users can access, modify, export, and delete their data
- Who to contact for questions or resolving issues
- Data protection and security
- Effective date of notice
- Changes to notice

Notice User Experience and Accessibility

Considerations

- Website content navigation
  - Can your patrons find the privacy notice on the front page of your site?
- Language
  - Jargon vs plain language
  - English as Other Language
- Audience
  - Cultural knowledge assumptions
- Notice accessibility
  - Accessibility standards and design best practices

Strategies

- Focus groups with staff and patrons
- Community listening sessions
- Usability testing – tasks to find and to interpret privacy information on the website
- Accessibility testing
- Translations
- Layered privacy notice design

Twitter is public and Tweets are immediately viewable and searchable by anyone around the world. We give you non-public ways to communicate on Twitter too, through protected Tweets and Direct Messages. You can also use Twitter under a pseudonym if you prefer not to use your name.

When you use Twitter, even if you're just looking at Tweets, we receive some personal information from you like the type of device you're using and your IP address. You can choose to share additional information with us like your email address, phone number, address book contacts, and a public profile. We use this information for things like keeping your account secure and showing you more relevant Tweets, people to follow, events, and ads.

We give you control through your settings to limit the data we collect from you and how we use it, and to control things like account security, marketing preferences, apps that can access your account, and address book contacts you've uploaded to Twitter. You can also download information you have shared on Twitter.

In addition to information you share with us, we use your Tweets, content you've read, Liked, or Retweeted, and other information to determine what topics you're interested in, your age, the languages you speak, and other signals to show you more relevant content. We give you transparency into that information, and you can modify or correct it at any time.

If you have questions about this policy, how we collect or process your personal data, or anything else related to our privacy practices, we want to hear from you. You can contact us at any time.

Communicating a Privacy Policy to Others

Privacy Policy

- Staff training
  - Interactive training
  - Refresher trainings
  - Scenario-based training
- Intranet knowledge base for privacy resources and documentation
- Email announcements
- Team meetings

Privacy Notice

- Marketing and Press Releases
- Community outreach
- Physical communication
  - Public posting in conspicuous areas
  - Pamphlets in service population languages
- Electronic communication
  - Website footer/header
  - (Maybe) Website alerts, emails, and “Just in Time” Notifications

What about vendor privacy notices?

The Santa Cruz Public Library System assesses each vendor we use for multiple data privacy and protection best practices. Each vendor is required to complete a Vendor Security Assessment Questionnaire, and respond to 78 questions in 7 areas:

- *Service Overview*
- *Data Protection & Access Controls*
- *Policies & Standards*
- *Application Security*
- *Compliance*
- *Security Measures*
- *Which Data Are Collected*

Product	Vendor
Academic OneFile	Gale
Acorn TV	RBDigital/Acorn TV
America's News	NewsBank

Exercise – Privacy Notice Review

Section Three: Procedures

Procedures vs Policy

- Policy is the “what” and “why” – high level, strategic goal; Procedures get to the “how, when, where, and who” of policy implementation
- Focused on specific areas and functions of the organization, including departments
- More responsive – can be quickly adjusted to accommodate changes and issues in daily operations
- Procedures = Documentation

Different Types of Procedures

- Law enforcement requests
- Patron data requests from:
  - Other patrons
  - Individual
- Staff handling of patron data, including collection, storage, and retention
- Incident response logistics
- Data sharing with:
  - Other departments
  - External third parties, including vendors

Privacy Procedures - Considerations

- Tying back to policy – built-in checks
  - Revision process for procedures – scheduled reviews, triggered reviews
- Writing with the audience in mind
  - Who will be using the procedures?
  - How will this procedure documentation be used?
    - Front desk staff dealing with a law enforcement request at the desk vs a planning meeting for a programming event
- Anticipating edge cases and other Unknown Unknowns
  - Short term and long term responses
  - Procedures vs Guidelines

Implementing Procedures

- Staff training
  - Interactive training
  - Refresher trainings
  - Scenario-based training
- Intranet knowledge base for privacy resources and documentation
- Departmental meetings
- Iterations and review schedules
- Language/script for staff to use for patron questions regarding policy/procedures

Exercise – Privacy Documentation in Action!

Section Four:
~~Reality~~ Practice

The best laid schemes of mice and men
Go often askew

~ Robert Burns, “To a Mouse”

The Staff Realities of Putting Policy and Procedure Into Practice

Communication

- Insufficient training
- Lack of clear organizational communication lines between staff
- Ineffective documentation - inaccessible, unusable by staff in particular situations – or lack of documentation

Things Outside Your Control

- Edge cases
- Rapid regulatory, technological, standards, and best practice changes

The Staff Realities of Putting Policy and Procedure Into Practice

Administration

- Lack of administration support for training, development, and enforcement
- Lack of resources, prioritization, and agency for privacy initiatives

The Human Factor

- Expectations to provide good customer service
- Being a helpful person and citizen

Patron Realities

Information overload from ineffectiveness of current practices

Increased surveillance and privacy risks for some patrons

Patron-Centered
Privacy Design

Good Design …

Honors Reality

Creates Ownership

Builds Power

Reflection – Design and Reality

Section Five:
Wrap up

What is one thing from this workshop that you can put into practice or discussion at your library when you return?

Thank you

:-)

Becky Yoose
Library Data Privacy Consultant
LDH Consulting Services

Email:
becky@ldhconsultingservices.com