Welcome back to the second week of the Data Privacy Best Practices Training for Libraries! This week we will cover all things data privacy training inside and outside the training room.
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.

This is a quick FYI that this workshop is part of a project supported by the Library Services and Technology Act, so thank you to the grant authority for providing resources for this project.
Today’s Schedule

10:00 – 10:15 Welcome and course housekeeping
10:15 – 10:45 Training
10:45 – 10:50 Break
10:50 – 11:25 Training
11:25 – 11:30 Wrap up

This privacy train the trainer webinar series runs on Wednesdays in March from 10 to 11:30. Each week we’ll try to keep close to the schedule posted in the slide. There will be some time for Q&A at the end of the session, so if any questions pop up during the presentation, you can enter them in the chat box so we can answer them then.
Last Week Recap

[Image description: a white, orange, and black calico kitten lays on a pile of newspapers on a red blanket.]
[Image source: https://www.flickr.com/photos/andres-y-linda/445989772/ (CC BY ND 2.0)]
We will be doing a good amount of discussion in this series and to help create an inclusive learning environment, I ask that everyone use this slide to help guide their interactions.

- When you disagree, challenge or criticize the idea, not the person.
- Speak from your own perspective. "I" statements are useful ways for keeping from generalizing about what others think or feel.
- We’ll have some time for discussion, but it’s always helpful to be mindful of the time while you are speaking.
- Online conversations can get busy quickly, so speaking one at a time can help mitigate confusion and overlapping conversations.
- This session will not be recorded, so you have some leeway as to what can be discussed off the record. Only attribute what is said in this space to an individual if they give you permission.
Reflection – That was the best/worst!

Think back to the best training workshop or class you’ve ever taken. What was the one thing from that training class that made it the best training you’ve had?

Now think about the worst training you’ve ever had. What was the one thing that made it the worst?

Save it for later!
1. WWWHW of Data Privacy Training

Alright! We’re going to start this week with the when, where, who, how, and what of data privacy training. Communicating that “why” to others in the library will be covered in week four of the series.
The When of Training

<table>
<thead>
<tr>
<th>Proactive Training</th>
<th>Reactive Training</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trainings that are regularly scheduled or part of an established process. Examples include:</td>
<td>Trainings that take place after a specific privacy-related event takes place, including after a privacy or security incident.</td>
</tr>
<tr>
<td>• Onboarding process</td>
<td>• This includes incidents outside your library, like other libraries or organizations (it’s a bit of a grey area on if this is a reactive or proactive approach, but still important to do!)</td>
</tr>
<tr>
<td>• Annual refresher trainings</td>
<td></td>
</tr>
<tr>
<td>• Other routine trainings and professional development opportunities</td>
<td></td>
</tr>
</tbody>
</table>

Let’s start with when. When’s the best time to train? There are a couple of ways you can approach when your training takes place.

Trainings that happen during the onboarding process, as well as other routine trainings, take a proactive approach to training. You can cover the basics in these scheduled trainings as well as deep dives into particular aspects of library data privacy. Refresher trainings help reinforce knowledge and could uncover some potential training needs with workers who already have experience implementing these policies and procedures. Having these scheduled trainings will help make sure that all workers will at least have passing familiarity with data privacy practices at the library.

There will be times where the need for training is triggered by an event. One example of this is a phishing or ransomware attack. Even when policies are followed, event-based training can positively reinforce behavior and knowledge. Think of a law enforcement request for patron data – that event in itself can make several staff anxious about making sure that they are following policy, and training can be one way to help with that anxiety. The event is fresh on everyone’s minds and there’s incentive to talk privacy while you have their full attention - attention that otherwise might not be there with scheduled training.

You’ll find that there are several types of privacy training that can be both proactive and
reactive. These could include implementing new processes, working with vendor products and services, and major changes to policies and procedures. Ideally you want a mix of scheduled trainings, impromptu trainings, and refreshers in your data privacy training program. There’s no magic ratio, but the one thing you want to avoid is to have your privacy training be all reactive training, coming in after a privacy incident and focusing on negative reinforcement.
Training Your Library Poll #1 – When?

Poll question – when does your library offer privacy training?

Poll options:
Once, when someone is hired
Annually scheduled trainings for all staff
When a privacy incident happens
Other (use chat box)
Remember in person training? It seems like it’s been ages since the last time I’ve trained folks in person!

Nowadays, training is online. However, for when we are able to choose where we hold trainings, it is still worthwhile to cover the strengths and weaknesses of each place.

In person trainings can create unique learning environments depending on the mix of people in the room. While lecturing is common, in person discussions and activities are popular in person teaching methods. One particular mode of learning that can’t be easily replicated online is the “hallway track” or the conversations that come up in breaks, or before or after the training session. However, in person trainings are limited by where and when they are held.

Online training can get around these limitations through asynchronous content delivery. You can pre-record lectures, assign readings, and have participants take quizzes or answer questions in discussion forums. You can build some opportunities for big and small group discussions, but most likely not replicate the hallway track mentioned earlier. Online training sessions can be synchronous, but that will run into the same schedule limitations as in-person trainings. Depending on resources, the software used for training can be a limitation for both the instructor and learner. One common example of this limitation is
software or training materials that are not usable with screen readers. Another limitation comes with transcription. I create a transcript for the slides, but that won’t catch people’s voice chats in the session.

Some of you might wonder about a hybrid approach. There have been in-person trainings supplement with online quizzes and discussions, and online trainings schedule in-person group discussions. Be aware, though, that it’s easy to combine the worst of both modes of training as well as the best. If you go with hybrid that there will be some who will not be able to participate in certain parts of the training, particularly if you do an in-person component to an online training.

[Image description: A adult white man juggling a variety of kitchen utensils, dishes and appliances in a kitchen.]
[Image source: https://www.flickr.com/photos/23119666@N03/6051513505/ (CC BY 2.0)]
Training Your Library Poll #2 – Where?

Even though the pandemic has pushed training online, where has your library traditionally held privacy trainings?

Poll options:
Online
In-person
Both
The Who of Training

- ALL library staff
- Library volunteers
- Library board members
- Organizational IT staff (outside library but within the overall organization)

Now that we covered the when and where – who do we train?

Ideally you want to train everyone who will come into contact with patron data. This includes working directly with data as well as working directly with patrons. Library staff and administration are pretty much givens, but we need to include library volunteers. Volunteers might not be aware of the patron’s right to confidentiality and privacy when they use the library, which includes asking questions about materials and resources, as well as attending programs and events. Volunteers also get questions from patrons about other patron’s checkout records, and they might even get asked for information from a law enforcement official. Training library volunteers about data privacy will at least make sure that volunteers are aware about patron privacy at the library.

Library board members and other external library governing bodies are another group that should be considered for training since they might have access to patron data through reports and discussions with the library. Training sessions to this group is also an opportunity to create privacy advocates on the board or governing body through illustrating why privacy in the library is critical.

The last group on the slide is one that comes from personal experience as a former IT worker and manager. The IT people you work with might not be in the library, but instead
campus IT or city IT. They most likely do not know the privacy policies, procedures, and practices around patron data. If your network, computer systems, web applications, or any productivity software and applications are maintained by those IT departments, then a conversation with key IT staff is a starting point in determining the shape and form of training for the IT department.

A takeaway from this slide is that your training should be tailored to your audience. Library board administration training and IT staff training will share some information, but these audiences most likely have different backgrounds, knowledge, and skills. We’ll talk more about this later in this session.

[Image description: A Zoom call screen with headshots of 13 adults of various races, ethnicities, and genders, as well as two call-in icons for two participants.]  
[Image source: https://www.flickr.com/photos/clender/50140285193/ (CC BY 2.0)]
Training Your Library Poll #3 – Who?

Who receives privacy training in your library?

Poll options – check all that apply
Library staff
Library volunteers
Library board members or other leadership
External IT staff
Other (use chat box)
2. Developing Training Content

Now we get to the interesting parts – what to include, and how to teach it!
It’s tempting to let the privacy training be a privacy policy readthrough. There might be times where, in the past, that was the only privacy training one received at the library. This section is going to push past that notion that a readthrough is enough for a training session. It’s not going to tell you exactly what to teach – trainings cannot be “one size fits all”. They need to consider the target audience and their needs. The trainer needs to set out learning objectives or goals for the training and how these objectives will be met. While we won’t have definitive answers for all of these questions for your specific situation, you will have a sense as to how to either create new trainings or revise existing trainings that meet the audience where they are at.
The most common privacy training topic is privacy policies and procedures. While this is appropriate for scheduled trainings such as onboarding new library workers and trainings for when policies change, you’ll quickly find that this only captures a small portion of your library’s privacy training needs. Library patron data is everywhere, and there are specific areas that require special attention or approaches in mitigating privacy risks. For example, teaching patrons about data privacy and security requires knowledge of basic data privacy and cybersecurity, including specific tools and practices. Working with vendors particularly in contracting and auditing require additional knowledge about industry standards and regulations around data privacy and information security. On the other end of the spectrum you might have board members who are very new to the library world and are not really sure how to articulate why people should care about privacy beyond the phrase “privacy is good!” while at the same time not understanding why library can’t just report on detailed demographic data of its users.

All of this will lead to different types of privacy trainings. Before you start creating all these trainings, however, it might help to think about needs. One place to start is the audience – you can make some educated guesses as to the level of knowledge and awareness they have about privacy at the library. If you aren’t sure what your library exactly needs, there are a few other ways you can solicit feedback from multiple audiences. Surveys tend to be the first thing that people use, and survey fatigue is real in libraryland. This is not to say that
surveys should be avoided, but they should be supplemented with other methods, such as coming to team meetings to discuss privacy concerns and interests. Coffee chats can be another option to talk one-on-one with an individual about their concerns about privacy at the library. You can also gather information from staff discussion areas, such as group email lists, discussion boards, and logs, and track any reoccurring themes and issues that might be good training topic fodder.
Choosing What to Cover

- Prioritizing learning objectives based on:
  - Audience
  - Organizational need
  - Knowledge/skill level
  - Time constraints
  - Training platform

- What can be covered outside of the training session and how?

There’s only so much time and recourses you can spend on privacy training, and you have to account for the fact that privacy training isn’t the only training library workers go through at the library. You might only get one scheduled slot in the training schedule of all employees. This is not ideal, and you should push for more scheduled training opportunities. For some of you, though, this might be all that you get.

Even if you have the option to create and teach multiple privacy trainings at your library, the temptation to cram everything into a single session is there, but that could lead to information overload or otherwise backfire. To help focus the training, you will need to do some prioritization work with your learning objectives for the training. How many of you are familiar with learning objectives?

[explain learning objectives if there are people who are not familiar]

Your learning objectives should reflect several factors, including your audience, time constraints, and the organizational need for that objective to be met by the audience. Another way to focus your training is determining which topics can be covered outside the training session. Training does not stop when the training session ends, and we’ll cover a few ways you can do this later in this session. This can help when you are having trouble narrowing down and focusing your training to fit within time, resource, or platform...
constraints.

[Image description: A black and white photo of a Black woman throwing one hand up in the air while reading a book, with a variety of books and laptops around her on a table.]
[Image source: https://www.flickr.com/photos/wocintechchat/25677271842/ (CC BY 2.0)]
Training Methods

**Lecture**
- Passive learning
- Ability to present a large amount of information in a short time
- Advanced preparation of training scripts and materials
- More control over training content and discussion
- Can be engaging, but limited
- No immediate feedback or application of material learned

**Interactive Methods**
- Active learning
- Learners can immediately apply what they learned in a semi-controlled environment and receive immediate feedback
- Learners can learn from their peers through discussion
- Relies heavily on learner motivation and participation

Another thing to think about is how you will convey these topics to your audience. The methods we choose in our training affect the learner’s relationship with that topic, including how they understand it and the motivation to understand it in the first place. Each method has its own set of strengths and weaknesses but you can use multiple methods in the same training to mitigate these weaknesses.

The two methods I have on the slide are from two types of learning: passive and active learning. What I’m doing right now is lecturing, which is a passive learning method. I’m dumping a lot of information on you, but it’s a way that I can introduce you to key concepts and topics in a controlled environment – aka the slides, scripts, and handouts. But information dumps don’t give you a chance to apply what you learned.

This is where active learning comes in. Interactive methods give learners the chance to immediately apply what they learned in the training environment. Learners can get immediate feedback from not only the instructor, but from their peers. One reason why some people love group discussions so much is that they get a chance to share and learn from their peers – I’ve had several people exchange contact information with each other after trainings as a result from a in-training discussion. This allows learners to practice what they learned and practice again and again, giving them experience that they can then draw on when they go back out to the field.
Active learning is great in that it gives learners that chance to reflect and apply what they just learned, but it’s only as effective as the most motivated learner. There have been times where no discussion happens and other times where discussion overtakes the lecture – it depends on who is in the audience, and how motivated they are to learn.
Types of Interactive Training Methods

• Group discussion (large or small)
• Games
• Exercises (individual or small/large group)
• Role play Scenarios

There are several ways you can give learners the chance to apply what they learned. Like surveys, group discussions tend to be the main choice of interaction. Assigning people to small groups and ensuring that people talk to different people instead of staying in the same small group are a few strategies to work through some of the pitfalls of group discussions. Having ground rules for discussions are also advised to mitigate conflict and power imbalances.

Games can be as simple as a custom board game similar to Candyland or Life or a pub trivia style event where there are teams playing for points to win a “fabulous” prize. In fact, practicing incident response processes in many fields takes the form of a table top exercise. There are also several published games in the marketplace that are specific to cybersecurity that you incorporate into trainings. Games will motivate folks who like competition, but be aware that some folks might get too competitive even with the simplest of games.

Exercises, like discussions, are commonly used in trainings. These could be a “what would you do in this situation?” problem or quiz. They can also be more elaborate. How many of you are familiar with Liberating Structures?

[explain LS if there are people unaware]
In Liberating Structures there are a few structures that can be turned into effective exercises. One is Trokia Consulting, where groups of three people act as both clients and consultants giving feedback to each other about an issue one member brings up. 1-2-4-All starts with an individual reflection on one question or topic, then pair off to discuss their reflections, then pair off with another pair of people to discuss their discussions, and then coming back to the entire group to share their discussions. These exercises can get the more quiet learners in the training an opportunity to contribute that they otherwise wouldn’t be able to in big group discussions.

Last, but not least, we have a method that people either love or dread, depending on what you call it. This method allows for learners to assume a particular role and try to work through a resolution or address a prescribed situation within a controlled environment. What I described just now is role playing, but you might have better luck with learner buy in with this method with an alternative name – scenarios.

[Image description: A group of nine adults of various genders, races, and ethnicities sitting on the grey carpeted floor or in a chair discussing with each other.]  
[Image source: https://www.flickr.com/photos/ironypoisoning/28134267271/ (CC BY SA 2.0)]


<table>
<thead>
<tr>
<th>Scenarios</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Objectives</strong></td>
</tr>
<tr>
<td>• What learning objective are you trying to achieve?</td>
</tr>
<tr>
<td>• What is the main takeaway for the participants?</td>
</tr>
<tr>
<td>• How does it tie back to the training material?</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

Incorporating scenarios into your training allows participants to put what they learned into practice with context that might otherwise be absent in other exercises and discussions. You will also find that scenarios can be a good way to get people to think about what they learned in a new angle or frame, or bring up questions that they otherwise wouldn’t have considered.

Building scenarios can an enjoyable experience if you like creating word problems or stories; nonetheless you will need to put some structure into their construction. Think mini lesson plan for those who had previous teaching or trainer experience. The objectives list on the slide are a good place to start in creating a scenario for training. What are the learning objectives, how does this tie back to the training material, and what is the main takeaway for the participants?

If you are stumped about what scenarios to create for your training, you can check shift logs and other library discussion forums for inspiration and for examples of past incidents. You can also model scenarios off of incidents that happened in other libraries. If you’re still not sure about what to write, or if you are not sure about your writing skills, there are several trainings that use scenarios that you can study and adapt for your trainings.
Your scenario framework will differ depending on how you plan to use scenarios. Creating a scenario for word exercises will differ from creating a scenario where the participants assume a role. On the slide are some questions and parameters to consider when creating a live action scenario for training. How many people will be in the scenario group will determine how many roles you have and what type. Sometimes you might want to assign one or two group members to be observers of the scenario and take notes about what happened. Creating material for the scenario includes the base text for everyone to read, specific text based on role, accompanying materials, and debriefing questions at the end for each group to discuss after they reached the time limit.

You can also bring the debriefing session one level higher by having an open discussion for the entire training class. Groups can then learn from each other and cover points or issues that other groups didn’t consider.

If it comes to the point where the groups are discussing everything except what you hoped they would learn from the exercise, that doesn’t necessarily mean that the exercise failed. It went in a direction that your learning objectives didn’t plan for. You can bring up some of the uncovered points through open questions to the groups. This is also an opportunity to learn from the groups’ observations and discussion to possibly tweak either the learning objectives/takeaways or the scenario for future trainings.
About those phishing tests...

Before we advance to the next section, I want to briefly address one other training method that has gained popularity in the cybersecurity field. You might have heard about people at other workplaces receiving questionable emails, only to find out that these were sent as a test to find out how many employees can spot phishing emails and other scams. These tests seem like a good idea because they can identify if there is a need for additional training; however, these tests can spectacularly backfire. For example, a library employee who is advocating for library workers to get the COVID-19 vaccine receives a phishing email about available vaccine appointments, only to find out that their library sent out the phishing test. If there’s one way to make your workers distrust IT or management, this example is most likely it.

The main takeaway from these stories of phishing tests gone wrong is that whatever training method you choose, you need to take into account the context of the training and the motivations that drive it. Negative reinforcement demotivates people to report suspicious emails or other possible security or privacy issues because they don’t want to be blamed for making yet another mistake. Positive reinforcement can help avoid staff creating additional risk to data privacy and security because of punitive approaches to learning and reporting.
[Image description: A screenshot of a news article titled "Do Fake Phishing Emails Really Teach People to Recognize Scam Messages?" accompanied by an image of a fishing hook piercing a envelope with a red circle with a dollar sign on the top right corner of the envelope.]
Discussion – ...now I know why!

Revisit the best/worst answers from the earlier reflection. From what we’ve covered so far, what would you do to improve the worst training?

For the best training, how could you incorporate what made it great into your own trainings?
3. Developing a Privacy Training Program

... or how to address common reasons why training programs fail

We got the training development down, now it’s time to figure out how to develop a sustainable training program at your library!
# Schedules and Resources

## Schedules
- Training schedules
- Onboarding checklist
- Setting a training date/time for refresher trainings
  - Scheduled informal discussions, coffee chats to supplement
- Time for training revisions and development, too!

## Resources
- Budget
- Apps or LMS for online training
- Professional development

As we mentioned before, you’re competing with other library trainings. Setting aside dedicated training times will at least ensure that library staff can access training during important times, such as onboarding and refresher trainings. Not all trainings have to be formal, either! Monthly coffee chats and other informal discussions can gather privacy advocates as well as the privacy curious into one space to discuss privacy at the library. You also need to schedule time to revise existing and develop new trainings.

For any training program to survive, the program must have resources, and financial resources at the very minimum. This support allows for professional development, such as train the trainer sessions where trainers can keep current on privacy trends, issues, and concerns. This support also provides the means to acquire training tools, such as a learning management system or interactive learning apps. This funding can also be used to bring in external trainers to train in particular topics that otherwise would not be covered in library trainings, such as data risk assessments or specific cybersecurity topics.
Training Team

• Several people or one person* depending on organization
• Dedicated training coordinator
• Instructors
• Training material reviewers/developers

* If you’re a one person shop, train staff to consult the training resources or knowledge base first before coming to you to avoid burnout

The other component in building a sustainable privacy training program is the people involved in training. You might have a dedicated training coordinator or a core group of trainers, or it might be that you ARE the training team. If you are a one-person shop, you will be swamped. Here you will need to train staff to do some due diligence on their end before coming to you for an impromptu training request. This does require some work on your end, but a little work now will save you a lot of work later. You can also train other people to lead specific trainings if you find yourself needing to conduct more trainings than the time you have available to teach.

We can’t forget that your training team is more than just your trainers. Other people in the training team include people who can review and beta test the training materials. This feedback can help focus workshops as well as catch any gaps or errors.

[Image description: Four cats sitting in a circle on a white shaggy carpet. A red and white stuffed toy fox lays between two of the cats in the foreground.]
[Image source: https://www.flickr.com/photos/christinehawks/50353121011 (CC BY 2.0)]
Discussion – The One Wish

If you can wish for anything in regards to privacy training and professional development at your library, what would it be?
4. Outside The Training Room

For the material that is left out of the training plan, you will need to find ways to bring that material to library workers.
Resources Outside of Training

- Knowledgebases (!)
- Documentation (!)
- Discussion areas (!)
- Blogs, news, social media feeds, conferences
- Other forms of professional development

(!) = essential for reinforcing or supplementing training

We discussed informal meetings such as coffee chats earlier on, but we cannot rely solely on these meetings as the main resource to support privacy training. Knowledgebases, documentation, and discussion areas are key areas to not only reinforce what workers learned at the training, but can also introduce topics that couldn’t be covered in the limited time of the training session.

External resources, such as blogs, news feeds, and conference recordings, are great resources to include in the library’s privacy documentation and knowledgebases in the form of a clearinghouse or another dedicated space for receiving current privacy news and developments.

[Image description: A white adult woman sits in front of an open laptop and notebook on a table with a black, white, and orange calico kitten sitting on her left arm on the table.]
[Image source: https://www.flickr.com/photos/mattbrowne/275140651/ (CC BY ND 2.0)
Nevertheless the way we communicate privacy to library workers matters just as much as the content that we communicate. For instance, we have to consider the ways that policy and procedure documents will be used in daily work. Sometimes staff need a quick guide to a lengthy procedure or policy when patrons are asking them questions at the information desk, or when a police officer is asking for patron information. FAQs, scripts, and handouts all can help staff to follow policy and procedure while not putting privacy at risk through not following these policies and procedures.

Updates about privacy practices covered in training as well as discussions about current practices can be covered in internal staff blogs and discussion groups where staff can contribute and observe. Meetings and emails are another way to convey privacy information; however, particularly in the case of email, your coverage may vary. Email tends to get missed or ignored. Meetings are not perfect, either, particularly when you come in to speak to a group who has a two hour department meeting. This shouldn’t stop you from using these formats to talk about privacy, but it’s worthwhile to ask what is the best way to convey this information to library workers.

[Image description: A brown and white tabby cat is sprawled on top of a Gateway keyboard, with a human hand reaching out to pet the exposed fluffy cat belly.]
[Image source: https://www.flickr.com/photos/89509548@N00/1070827696/ (CC BY ND]
Questions and Open Discussion
Wrap Up
Next Week

**Week Three - Beyond Data Privacy Training**
- March 17th, 10 am – 11:30 am

**Week Two Activities/Reading**
- Skim through the slides and handouts of Year One trainings
- Other trainings listed in Year One toolkit, Section 7 under “Other Library Privacy Trainings, Programs, and Courses”
- Exercises on Basecamp
Thank you
:-)

Becky Yoose
Library Data Privacy Consultant
LDH Consulting Services

Email: becky@ldhconsultingservices.com

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
Resources and Further Reading

• “California Government Code § 6267. Registration and Circulation Records of Library Supported by Public Funds.”
  https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=6267&lawCode=GOV.

• Center for Educational Innovation. “Active Learning.” University of Minnesota.

• Center for Teaching Innovation. “Active Learning.” Cornell University.
  https://teaching.cornell.edu/teaching-resources/engaging-students/active-learning.

  https://teaching.cornell.edu/teaching-resources/designing-your-course/setting-learning-outcomes.

Resources and Further Reading


Additional bibliographies and resources can be found in the Toolkit and training resources at the https://www.plpinfo.org/dataprivacytoolkit/.