ALA American Library Association

CREATING ADAPTABLE DIGITAL PRESERVATION WORKFLOWS

Erin Baucom

Library Technology Reports
Expert Guides to Library Systems and Services

MAY/JUNE 2021
Vol. 57 / No. 4
ISSN 0024-2586

Library Technology
REPORTS
Expert Guides to Library Systems and Services

Creating Adaptable Digital Preservation Workflows

Erin Baucom

ALA TechSource
alatechsource.org

American Library Association

Library Technology
REPORTS

ALA TechSource purchases fund advocacy, awareness, and accreditation programs for library professionals worldwide.

Volume 57, Number 4
Creating Adaptable Digital Preservation Workflows
ISBN: 978-0-8389-4824-8
DOI: https://doi.org/10.5860/ltr.57n4

American Library Association
225 N. Michigan Ave., Suite 1300
Chicago, IL 60601-7616 USA
alatechsource.org
800-545-2433, ext. 4299
312-944-6780
312-280-5275 (fax)

Advertising Representative
Patrick Hogan
phogan@ala.org
312-280-3240

Editor
Patrick Hogan
phogan@ala.org
312-280-3240

Copy Editor
Judith Lauber

Production
ALA Production Services

Cover Design
Alejandra Diaz and ALA Production Services

Library Technology Reports (ISSN 0024-2586) is published eight times a year (January, March, April, June, July, September, October, and December) by American Library Association, 225 N. Michigan Ave., Suite 1300, Chicago, IL 60601-7616. It is managed by ALA TechSource, a unit of the publishing department of ALA. Periodical postage paid at Chicago, Illinois, and at additional mailing offices. POSTMASTER: Send address changes to Library Technology Reports, 225 N. Michigan Ave., Suite 1300, Chicago, IL 60601-7616.

About the Author

Erin Baucom is an associate professor and the digital archivist at the University of Montana. She is responsible for developing strategies, workflows, and policies for ingest, management, and preservation of born-digital materials acquired archives. She provides digital asset management instruction to the students, faculty, and staff of the university. She earned her master's degree in library science with a concentration in archives and records management from the University of North Carolina at Chapel Hill in 2016. She also holds a BA in history from Old Dominion University.

Abstract

Libraries are scaling up their digitization, digital scholarship, digital archiving, and data management programs. All of this effort could be lost to a major failure of technology, a shift in administrative priorities, or a loss of institutional memory. The loss would not just be the materials themselves, but also the resources used to build and promote these collections to users. This issue of *Library Technology Reports* (vol. 57, no. 4), "Creating Adaptable Digital Preservation Workflows," will help libraries create transparent and enduring digital preservation workflows that will help them maintain consistent and transparent practices when acquiring, accessioning, stabilizing, processing, providing access to, and preserving their digital materials.

Subscriptions

alatechsource.org/subscribe

Contents

Chapter 1

Introduction

In Montana, we have the Treasure State Academic Information and Library Services (TRAILS) consortium. Its main purpose is to leverage collective purchasing power and facilitate collection sharing of library resources. However, TRAILS has provided a platform for other professional collaborations, one of which is the Digital Preservation Committee (DPC). In the DPC, librarians from various academic libraries around Montana meet and discuss issues related to digital preservation. We try to start our conversations with an update about the current state of digital preservation at each participating institution. Often, most of the librarians don't have an update; they don't consider what they do to be digital preservation. However, when we delve deeper, each individual has taken concrete steps toward preserving at least some digital material. This disconnect between what my fellow librarians and archivists see as digital preservation and what they are already doing can often be attributed to the fact that there is a continued misconception of what digital preservation is and what it takes to do the work of preserving digital objects.

These misconceptions can be, in part, attributed to the fact that digital preservation is still a relatively young field and is constantly evolving. There are no clearly established pathways and formulaic processes to follow as there are in other library and archives practices, such as cataloging. A further complicating factor is that what is currently available to guide digital preservation practitioners has been purposefully written to be high-level and general so that the guidance can be followed by as many different types and sizes of institutions as possible. However, for many librarians and archivists who have had digital preservation responsibilities added to their existing workloads, translating general guidance into step-by-step actions has been a difficult endeavor. Helping librarians and archivists make the transition from theory to practice is what workflow documents are meant to do. These workflows are some of the missing puzzle pieces that institutions, like my fellow TRAILS members, need to understand that what they do *is* digital preservation and to help move their digital preservation efforts into a more robust and sustainable program.

Digital preservation workflows are, in their simplest form, a list of steps taken to preserve digital materials and their accompanying metadata for future researchers to access. The act of documenting what steps you are taking to do these processes performs several functions. The first is to create a living document that provides a set of instructions for those working with digital materials to use so that the processes are done in a consistent manner. The workflows guide users through a set of decision points allowing the same document to be used regardless of the format the digital material takes. This streamlines processes and provides clear guidance on who to contact when problems occur. Second, these workflows are a way to document institutional memory so that work does not stop if key personnel leave the institution. Finally, documenting a workflow as it currently exists illuminates the current priorities and biases of an institution. Carefully examining existing workflows will allow you to reprioritize efforts and actively address those institutional biases.

Recently, the digital preservation community has encouraged institutions to document and share their existing practices to help make this translation from theory to action into a viable process for libraries of all types and sizes. In this report, I will discuss how to document your existing practices, examine that documentation for gaps and biases, and provide examples of digital preservation workflows for common stages in the digital curation life cycle—from donor engagement, accessioning and stabilization of digital materials, and processing these materials to providing researcher access and maintaining the digital content over time. While these workflows are based on the current workflows used at my institution, I will also provide tools and strategies for you to adapt these workflows to be useful for your particular institutional context.

Chapter 2

Workflow Basics

What a Workflow Is

Before diving into digital preservation workflows and processes, I want to take some time to explain what I mean when I use the word *workflow*. In its simplest form, a workflow is a series of steps taken to complete a task. A workflow can be so practiced in our personal and professional lives that we often don't even realize that we are following one—that is, until we try to teach someone else how to complete the task we have created the workflow for. A cooking recipe is a great example of this. My mother has this amazing chocolate mousse recipe that she cooked by rote, with no written instructions. However, when I asked for the recipe, it took her four attempts to successfully make the mousse, before she could translate the recipe from her brain to paper. We learned our lesson. The next time we needed to write down one of her mental recipes, I watched her and wrote out exactly what she was doing as she did it. This helped her not be distracted by trying to do two completely separate processes at once, cook and document what she was cooking. We all have professional workflows just like this. Just as in this example, we may need a little help documenting these workflows.

Workflows can be high-level and theoretical, or they can be simple and concrete. The high-level workflows are extremely useful when describing multiple interrelated processes that must be performed to complete a task. High-level workflows are also useful when creating documentation to share with fellow institutions, when trying to advocate to administrators for resources, or when teaching broad concepts. An example of a high-level workflow in digital preservation is the Open Archival Information System (OAIS) reference model.[1]

This is a purposefully abstract model so that it can be used by any size or type of institution to develop a digital preservation program. The model describes how to package information received from a creator, stabilize it, process it, and provide it to an end user. The model also documents the understanding that these steps are encapsulated by an ecosystem of preservation planning and administrative management required for a preservation program. How these high-level processes, plans, and management are achieved is left completely to the institutions implementing the OAIS model.

Low-level workflows are like the recipe I mentioned. They are a series of steps, most often written as instructions, that are followed the same way every time so that tasks are completed in an efficient and consistent manner. I describe these workflows as low-level, but that does not necessarily make them simple. It just means that the documentation describes the process in such a way that implementors need to make few, if any, independent decisions when following the workflow.

I will say that not every process will be able to be broken down into a low-level workflow. The more human interaction required in a process, the more likely the workflow will need some level of abstraction. The abstraction allows implementors to respect the needs and wishes of those they are working with to complete the task described by the workflow. An example of where abstraction is important in a digital preservation workflow is any process that involves a donor, creator, or end user. These abstract workflows are most commonly part of the pre-accessioning/acquisition phase and the access phase.

Why Documenting Workflows Is Important

I make the distinction here between workflows themselves and documenting workflows because I want to emphasize that we all have workflows for the processes we do every day. These workflows are so practiced that they are unconscious processes, to the point

that we don't even notice when we tweak and change how we perform the tasks. These changes happen to make the steps in the workflow easier or because a new skill was learned or a new tool implemented that makes the workflow more efficient. Without documentation, it is difficult to remember when and why the changes to the workflow occurred, which, among other complications, introduces a lack of transparency into the processes performed.

Documented workflows are evidence of past and present practices that create transparency, provide an audit history of processes and tools used, and prevent institutional memory from being concentrated in one person. Like any other design process, documenting and using workflows is an iterative process that changes over time. Having versioned documents tracks those changes. This can be especially important in digital preservation because if errors or corruptions occur in digital materials, knowing how these materials were treated in the past increases your ability to retrieve a clean copy of the materials affected to replace the corrupted content.

Beyond the everyday use of workflow documents, which is to perform processes consistently and efficiently, there are advocacy, educational, and relationship-building functions of documented workflows. Having workflow documents you can share with an institution just starting out or trying to ramp up its digital preservation program increases your ties to that institution and saves it time and resources it would have spent reinventing the wheel. Examining your workflow documents allows you to take a critical look at your processes to determine if there are gaps, outdated practices, or even institutional biases that need to be remediated. Examples of institutional biases include how processing priorities are assigned, which donors are approached for potential accessions, and how open the archives are to community input in arrangement, description, and access decisions. Finally, being able to share your workflow documents, or your analysis of your workflows, as evidence to support an argument for new resources or potential policy changes with administrators and funders can increase the likelihood that these advocacy efforts will succeed.

How to Document Existing Workflows

There are many ways to document a workflow, including visual diagrams, outline style instruction lists, paragraph style narratives, and spreadsheet style checklists. For an existing process, my favorite place to start is with an empty surface. I recommend a whiteboard or a very large presentation notepad and a pile of sticky notes. The beauty of this method is that it works for someone doing this process alone or for a group of people working together. On the sticky notes are written all of the steps in the process. If the surface used is a wall or some other material that does not allow for erasable writing, sticky notes can also have directional indicators, such as arrows, on them. After you think you have all your steps written on individual sticky notes, place the notes in the order that you perform the tasks, either drawing arrows to indicate the direction of the steps or using other sticky notes as directional indicators. The beauty of the sticky notes is that they are easy to reposition. This is an essential function because it is very rare to get the documentation correct on the first pass. The sticky note method also allows you or your team to set aside disputed steps to come back to later. This makes it more likely that you will be able to focus on the bigger picture of the entire process instead of hyperfocusing on a single step. This method, heavily focusing on teamwork, is more fully explained in "Process Mapping as Organizational Assessment in Academic Libraries" by Sarah Barbrow and Megan Hartline.[2]

This is only one example of how to translate current processes to paper. Other methods are described in "OSSArcFlow Guide to Documenting Born-Digital Archival Workflows," which includes a questionnaire that delves into *why* you are currently taking the steps you take and if the priorities driving your current efforts are the priorities you want guiding future iterations of your workflows.[3]

Whatever method you use to document your workflows, the process should be done for all the workflows you do not currently have documentation for. Importantly, even if you have current documentation for all your workflows, you could use these processes as a way to step away from your current documents and reexamine your workflows.

When working through these efforts, you may find that you want to start in the way this report has modeled, with a high-level document that simply lists out the various stages of the archival process: developing a relationship with a donor or creator, acquiring a collection, accessioning, appraisal, arrangement and description, providing access, and continual maintenance of the materials. Then break down each of these processes further into a series of more detailed workflows until you are satisfied that the tasks cannot be further differentiated from one another.

Your situation will determine who is involved in the documentation effort. As the digital archivist at a small archive, I can do almost the entire process on my own with some consultation with the head of the archives regarding donor relations and the information technology department regarding the tools and systems I do not have complete authority over. At a much larger institution or an institution of the same size with a different organizational structure, this

process will involve multiple people and will therefore take longer and include more complex workflows because the materials change hands at different stages. A high degree of collaboration is essential to creating an accurate document, even though the documentation process may take longer and involve several negotiations over how the processes are documented.

It is vital to be completely honest about your current process. The purpose of the documentation, at this stage, is to create evidence of what you do now. It is not meant to document your ideal process or the standard process espoused by, in this case, the digital preservation community. An honest documentation of your current workflow is the only way to truly understand what you are currently doing, where your gaps and your priorities are, and how your resources are allocated. Only after creating this honest workflow can you determine where effective and efficient changes can be made.

Notes

1. Brian Lavoie, *The Open Archival Information System (OAIS) Reference Model: Introductory Guide*, 2nd ed. (Digital Preservation Coalition, 2014), https://doi.org/10.7207/twr14-02.
2. Sarah Barbrow and Megan Hartline, "Process Mapping as Organizational Assessment in Academic Libraries," *Performance Measurement and Metrics* 16, no. 1 (2015): 34–47, https://doi.org/10.1108/PMM-11-2014-0040.
3. "OSSArcFlow Guide to Documenting Born-Digital Archival Workflows," Educopia Institute, June 23, 2020, https://educopia.org/ossarcflow-guide/.

Chapter 3

Acquisition Workflow

Building Relationships with Donors and Creators

In many cases donors and creators are one and the same, but that is not a universal truth. In terms of digital material, engaging with creators is almost more important than working with a donor, especially if they are separate entities. The creators provide vital contextual clues that are much more hidden in digital materials than traditional paper materials. Creators control how files are created, named, and arranged in their original operating environment. All of this has a direct effect on if and how digital materials can be preserved and provided to researchers in the future. The earlier you can build a relationship with a creator, the more likely it is that digital materials will survive to be used by a future researcher.

Beyond the technical and contextual aspects of digital preservation, there are strong ethical reasons for engaging donors and content creators frequently during the entire process. This engagement can prevent archival silences and the biases of archivists affecting the appraisal, arrangement, and description of the materials. Engaging donors and giving them direct power over how their materials are preserved, described, and provided to researchers ensures that trust is maintained with the donors and that more perspectives and voices are represented in the archives.[1]

Also, due to emerging post-custodial concepts, it may be that materials never directly enter your archive. That does not mean that these workflows are made obsolete. Instead, it will be your responsibility to adapt the workflows to fit a model of shared custody or to use them as a tool to teach community archives how to maintain and provide access to their digital materials. The key to digital preservation is adaptability. At this stage, you will have to adapt to the needs, cultural and personal, of your donors to ensure that the digital materials they create are integrated into the archival record.

The Importance of Informed Consent

Engaging with donors and creators allows you to ensure that they are fully informed about the ramifications of donating digital materials that will eventually be available to researchers. Informed consent is a concept that I first encountered in medicine, but it is also commonly found in research. It has also been an issue more recently in disclosure of personal information gained by companies like Facebook when users interact with their services. In medicine in many countries, informed consent is a legal right that patients have. It mandates that all the risks and benefits of medical intervention be explained to a patient in a manner that the patient understands before the patient legally agrees to the procedure. I will say that this is the intent of informed consent. In practice, some explanations patients are given are similar to the terms and conditions forms consumers are asked to agree to before downloading an app, seemingly written in a different language. There has been a strong push by patient and consumer advocates to mandate that the way in which informed consent is achieved be simplified to make sure that those affected truly understand what they are risking (or giving away) in return for the service received.

Informed consent applies to digital preservation in many different ways, including how materials are retrieved from donors, preserved by archivists, and made available to researchers. Personally identifiable information and clearly private information that can

be easy to spot in paper materials can be hidden in the metadata and system files of digital materials. Donors are often not aware of this hidden data or even the amount of data that can be pulled off a device through digital forensics or that is present in underlying metadata in files that were directly copied from the donor's operating system.

Gaining informed consent from your donors about what they are donating and potentially providing future researchers access to is a critical aspect of the donor engagement process and the acquisition workflows. There are various strategies for ensuring that donors clearly understand what they are agreeing to. These strategies are adaptable to a donor's demonstrated level of understanding of the technical aspects of digital preservation. The ultimate goal is to disclose to donors all pertinent information regarding the donation of digital materials, including the possibility of disk image creation and digital forensic analysis, in a manner the donors can understand. Ideally, you would have a donor demonstrate this understanding in some manner before signing a deed of gift that explicitly includes sections related to digital materials that the donor must agree to separately.

I have developed a list of goals for ensuring that I have done everything possible to achieve informed consent:

- The donor is aware that digital materials will be transferred as part of the donation and that it is possible that a disk image may need to be created and digital forensic analysis performed.
- The donor is aware that they can restrict access to all or a portion of the digital material, disk image, and digital forensic reports.
- The donor is aware that they can refuse to allow a disk image to be created or digital forensics to be performed.
- The donor has shown me that they understand the information that can be found within digital materials, disk images, and digital forensic reports.
- The donor consents to the final agreed-upon digital preservation plans for their materials, in writing.

The mechanisms that help me achieve these goals include

- a deed of gift with a section dedicated to the unique permissions required for digital materials
- a donor interview, a donor survey, or both regarding the creation and use of their digital materials
- a demonstration of where information is hidden in individual file metadata and file system metadata overall and the kinds of information that can be found within the reports generated by digital forensic analyses
- providing donors with all policies and procedures regarding digital materials and carefully walking through how those policies and procedures would apply to the donor's materials

It may seem like a lot of up-front work with donors before materials are ever acquired by your institution. However, these interactions only increase the trust your donors will have in your institution and in your abilities to provide long-term access to the materials. This work, especially the donor interview and survey documentation, will also help you when you later arrange and describe the materials. Finally, the documentation provides you with legal protection because you have generated evidence of the donor's knowledge and consent to all the agreed-upon preservation actions.

To be clear, this engagement is not limited to donors from outside your institution or institution members who are providing personal materials to your archives. It also applies to content creators within your institution who are transferring records to your archive according to a records retention schedule or other internal policies and procedures. In the case of internal records creators, the engagement should happen as early as possible so that the records are being created using consistent file formats and standardized file naming and file organization practices whenever possible. These creators also need to be aware of what can be hidden in files. Despite the best intentions and efforts of organizations and employees, often a creator's personal material can be accidentally included in organizational materials transferred to the archive. Constant communication before and during transfer can help reduce the chances of this happening.

Depending on your institution's staffing and organizational makeup, it may be that you are not working with the donor directly. In that case, you will need to work closely with the curator, archivist, or representative who interfaces with the donor so that as much of this process can be done as possible. How you approach this will depend upon your organization's culture and priorities. You may need to lean on the legal risks associated with not following these procedures. You could emphasize the contextual documentation generated through these procedures that would make the eventual processing of the collection more efficient. You know what avenues of advocacy work best for your organization. Leverage that knowledge.

Acquisition Workflow

The acquisition workflow (see figure 3.1) determines if materials should be acquired, documents interactions with donors before materials are transferred,

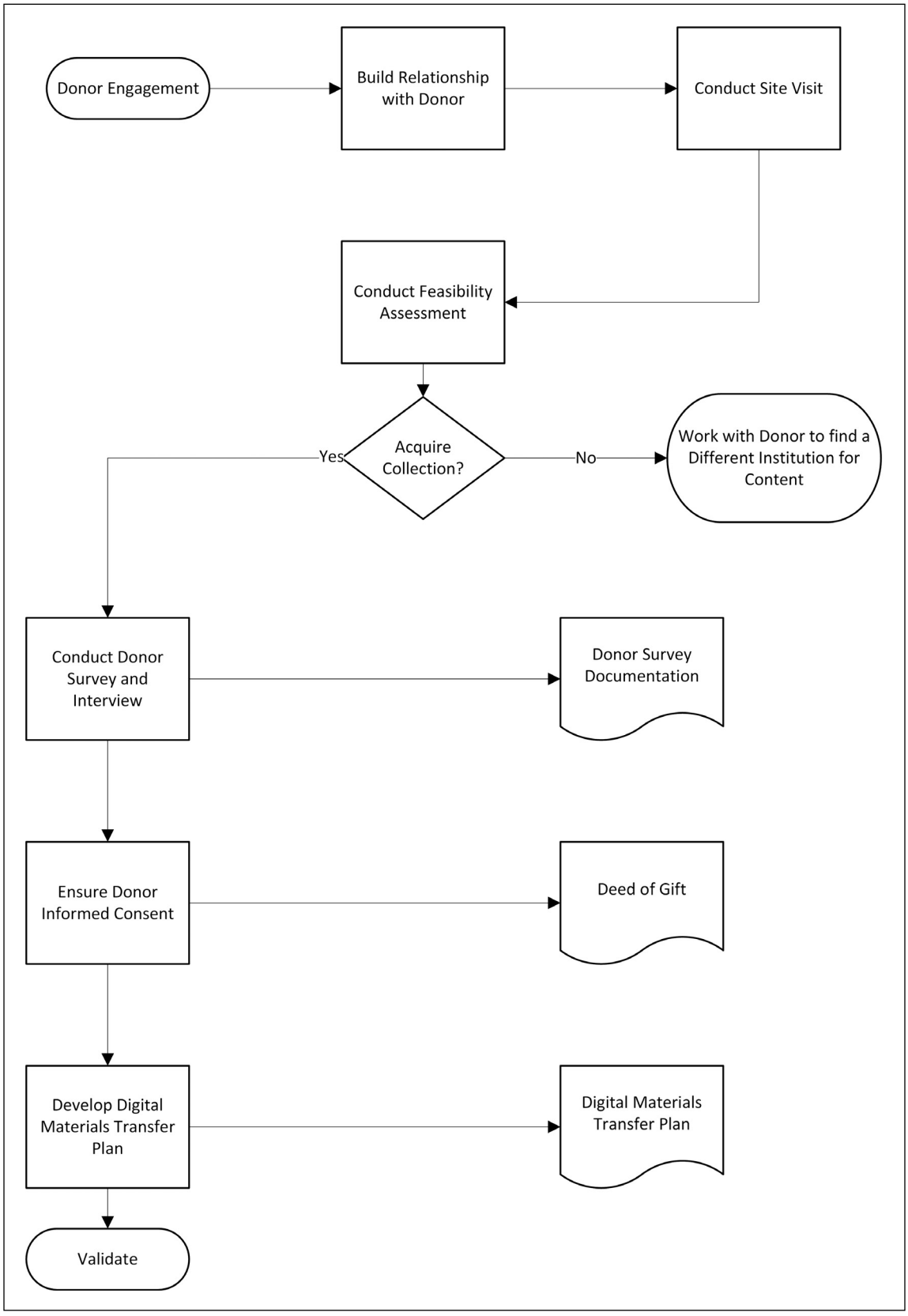

Figure 3.1
High-level workflow diagram of the acquisition process

and describes the actual transfer of materials from donor to your institution.

Feasibility Assessment

When your donor is ready to start discussing a transfer or donation of materials to your institution, before moving forward with any other steps, you need to determine if it is feasible for you to accept the materials. The first half of this feasibility assessment is determining that the digital materials are within the collecting scope of your institution. The second half of the feasibility assessment focuses on answering this question: "Do we have the time, expertise, and resources to responsibly curate the materials being offered to us?" If you currently have all the necessary resources, then you move along in the workflow. If you do not, you must then determine if it possible to advocate for and realistically receive the additional resources needed to preserve and make available the offered digital materials in the long term. If not, I encourage you to work with the donor to find another institution that has the interest and ability to preserve and provide access to the materials.

The feasibility assessment is solely focused on your institution's *current* infrastructures and resources in relation to the digital material being offered by the donor. Remember, this assessment is being done without doing a deep dive into the materials, just with the general information provided by the donor or discovered in a brief site visit.

ASSESSMENT QUESTIONS

- Are there file format types within the donation outside your current abilities to preserve?
- Is the size or volume of the collection beyond your current storage and preservation management capacities?
- What is the likelihood that content is corrupted, unstable, unreliable, or incomplete?
- Is there content that requires specific software platforms to render and make accessible that you do not currently have access to? If you do not have those resources, is it feasible to acquire and maintain the software needed?
- Is preservation of original physical media carriers required or necessary?
- How feasible and practical are ongoing transfers of data, if needed?
- What are the potential needed migrations and transformations? What are the anticipated costs of those migrations and transformations?

It is your overall evaluation of all these questions that will determine if it is feasible for you to acquire the collection. Each question will be weighted differently depending on your own institution's resources and priorities. For those acquisitions you choose to move forward with, the answers to the questions above can be incorporated into your donor survey or donor interview documentation.

Donor Survey and Interview

The ideal scenario is to pair the donor survey with a follow-up interview so you can tease out the most information possible. A conversation, instead of simply reading and responding to the text on the page, can help jar memories loose and help donors better understand the questions in the survey. The survey could be shorter or longer than the example I provide. It all depends on the types of materials your institution collects, the priorities you have regarding documenting collections in context, and what each donor is offering.

CREATION

Determine copyright and intellectual property ownership and dates of creation:

- Does your collection contain e-mail, documents, or other materials produced by others?
- If so, who else created content included, and what are their roles?
- What are the earliest dates of file creation?
- What are the latest dates of file creation?

CONTENT

Determine content types, file format types, and duplication of content in paper and digital formats:

- What types of content do you create: correspondence, journals, research notes, preservations, reports, photographs, sound recordings, videos, research databases, others?
- What types of digital files did you create: word processing, spreadsheets, images, databases, websites, others?
- Is there content that exists in both paper and digital form (such as print outs of word processing files)? Can you identify this content?

ORGANIZATION

Determine naming scheme for files, organization and ordering of files, frequency of file destruction, and storage of files on multiple devices:

- How are digital files named?
- Do filenames indicate if the file is a draft or final version? How is this indicated?
- How are digital files organized?

- Are personal files stored separately from work files?
- Are digital files destroyed on a regular basis?
- Is more than one computer used to create and store digital files? Remember that a computer could be a tablet, phone, or an actual PC.

E-MAIL

Determine use and organization of e-mail (if included in the donation):

- Do you have multiple e-mail accounts?
- What e-mail programs and services do you use: Microsoft Outlook, Mac Mail, Hotmail, Gmail, Yahoo! Mail, others?
- How is e-mail organized?
- Do you create folders or labels to organize?
- How is e-mail saved: stays in the e-mail program, copy saved to computer, paper printout, others?

PRIVACY AND SECURITY

Determine files that may require restriction, need for passwords to view files, use of other encryption methods:

- Do some files contain sensitive or confidential information?
- Are there specific files that you would want temporarily restricted or permanently removed or destroyed?
- Do any files require passwords to open?
- Where are usernames and passwords located? Do you use an external service to manage usernames and passwords?
- Are any other encryption methods used to protect files?

STORAGE AND BACKUP

Determine existence of backup procedures, storage of files on different media, and incidents of lost or damaged files:

- Do you regularly back up your files?
- Does someone assist you with technical support?
- Are your files automatically backed up? By your institution?
- What media are used for backing up files: optical disk (CD/DVD/Blu-ray), hard drive, file server, web backup service, other?

TECHNICAL

To be documented by archivists after conducting physical review of technical environment:

- What are the hardware configurations for each computer or device?
  - manufacturer
  - model no.
  - CPU
  - RAM
  - hard drive capacity
  - video card
- What operating systems are used?
- What other system software is used?
- What are the main software applications used to create digital files?
- Is "user" for software applications set to name of creator/donor?
- Are computers connected to a network file server? Is file server space used by creator/donor?
- Are login username and password required to access computers?
- What is the total size of digital files to be donated?

Deed of Gift

Depending on your organization's acquisition and accessioning procedures, this piece of the process may come earlier or later than where I have it listed. However, I encourage you to have a separate section in your deed of gift or transfer agreement document to directly address digital materials. Here is some language to consider or use as an example for additions or modifications to your existing deed of gift or transfer agreement templates.[2]

SENSITIVE INFORMATION AND ACCESS RESTRICTIONS

Some or all of the collection may contain sensitive materials and require access restrictions. It is *Donor's* responsibility to outline all restrictions that must be placed on which specific materials, who is allowed to have access to the materials during the restriction period, and when the restriction period expires. All restrictions *must* have an expiration date, or the materials will not be accepted. Either below or in an attached document, please list the specific materials (device, folders, and/or individual files) to be restricted and the conditions regarding the restrictions.

CREDENTIALS AND PERMISSIONS

If the collection contains digital materials that are protected by passwords, logins, encryptions, or other restrictions, *Donor* grants *Institution* permission to use to use passwords, logins, or other access keys *Donor* will provide in order to access the collections. If *Donor* declines (does not remember/have the ability) to supply passwords, logins, or other access keys for *Institution* to access digital materials that are protected by passwords, logins, encryption, or other restrictions,

Donor authorizes *Institution* to decrypt passwords or encryption systems, if any, to gain access to data received as part of the collections. If *Donor* does not authorize *Institution* to decrypt passwords or encryption systems to gain access to data received as part of the collection, then *Donor* agrees that *Institution* will discard these materials.

DISK IMAGING

Disk imaging is one of many established practices used by archivists to preserve materials. A disk image is a sector-by-sector copy of data that replicates the structure and content of data. *Donor* acknowledges that forensic imaging procedures may uncover information that was once deleted or overwritten by *Donor* and that imaging procedures may be used by *Institution* to preserve the collection in accordance with standard archival practices. By donating the collection, *Donor* grants *Institution* permission to use imaging procedures in order to preserve the collection.

Disk imaging may recover deleted files, log files, system files, and other files that document use of computers or systems. Does *Institution* have your permission to perform disk imaging?

If disk imaging is performed, does *Institution* have your permission to provide access to deleted files if they are recovered?

If disk imaging is performed, does *Institution* have your permission to provide access to log files, system files, and other files that document use of computers or systems if they are recovered?

Develop a Digital Materials Transfer Plan

To develop a digital materials transfer plan, you will pull heavily from the donor survey or interview mechanism. The digital materials transfer plan is meant to document the decisions made by you and the donor regarding what materials will be transferred into the custody of your institution and how that transfer will take place. This transfer plan may be determined through a series of e-mails, a simple verbal conversation, or a surprise drop-off at your institution. Any agreements should be documented in some way and included in the master file for the donation, whether through printouts of e-mails or written summary of phone or in-person conversations. Alternatively, you could document the transfer using a formal mechanism similar to the digital materials transfer plan. However transfer occurs, all of the following (or as much as is possible to collect) should be documented.

DEFINE INFORMATION

- Content types to be transferred.
- Types of software, operating systems, and other technical infrastructure that were used in the creation and management of the digital materials.
- Indicate if, and in what form, descriptive information about the digital materials exists.
- Indicate formats to be transferred. (Do not try to create a detailed list; just provide enough information to give a general idea.)
- If there are physical media items to transfer, create an inventory that indicates each type of electronic media and how many of each type are to be transferred.
- If only data is being transferred, indicate the total data size to be transferred.
- Describe the specific file-naming conventions or rules used to identify materials. Indicate if filenames are based on specific best practices or standards.

DEFINE TRANSFER PROCESS

- Packaging
  - Determine who will be packaging—donor, archivist, or donor and archivist together.
  - Determine if this is a one-time transfer or if there will be additional future transfers, scheduled or otherwise.
  - Determine type of transfer: physical only, logical only, combination of physical and logical.
- Transfer method
  - Determine how packages will be transferred:
    - Physical transport of electronic media as-is. No data or files copied from original electronic media.
    - Data transferred from local machine or network to archivist's portable device and physically transported to archives.
    - Data transferred via network or internet.
    - Data transferred from local machine or network to donor's or creator's portable drive or electronic media and transported by donor or creator to archives.
  - If data is being transferred via network or internet, test the transfer method and schedule a time for the transfer, making sure to allow for potential problems during transfer that might necessitate starting the process over.
- Tools
  - If retrieving data from the donor's or creator's device or machine to a portable drive, determine the hardware you will use for the transfer and what software tools you will use to do the data transfer. Potential transfer software tools include
    - Exactly
    - Data Accessioner
    - TeraCopy[3]
  - If the data is being transferred via network or

internet, determine what software will be used to transfer the data and that the donor understands how to use the software and has practiced using it. Ideally the data will be packaged using a software tool such as Exactly and then sent via secure network transfer protocols or a secure online file-sharing service such as Box.[4]

DEFINE VALIDATION

- Verify
  - All components (digital objects and metadata and all electronic media) were transferred.
  - Components are well-formed and were not corrupted during transfer.
  - Components are free of viruses.
- Acceptance
  - All initial validation requirements are met. This requires that components have been inventoried and (when data is transferred along with physical media carriers) checksums generated before transfer, which may not be possible for all transfer scenarios.
  - Some validation requirements are met. Acceptance criteria for transfers where full packaging (inventory, checksums generated) has not occurred before transfer may need to be flexible in response to different transfer scenarios.
  - Repeat transfer. There are likely to be transfer scenarios where some amount of data has been corrupted or files infected by a virus. Determining whether to accept such a transfer and report errors or to not accept and attempt a retransfer should be decided on a case-by-case basis.
- Tools
  - Determine validation software. Validation software should have the ability to
    - verify package contents contain all components
    - verify package contents are well-formed
    - verify package contents are free of viruses
    - produce validation report
  - Many transfer tools also act as validation tools, such as Exactly, DataAccessioner, and TeraCopy.

Transfer Materials

Follow your digital materials transfer plan. Each transfer will be more or less complicated depending on the amount of material to be transferred and the type of transfer occurring. The simplest transfers are of physical media carriers alone: you inventory the items before transfer and verify that the same number and type of items arrive at the archive. The most complicated transfers are hybrid collections, where paper materials, physical media carriers, and data are all transferred as one accession. These transfers must be carefully documented, and post-transfer verifications must be thorough so as not to disassociate any data from the other parts of the transfer. It is crucial to move directly to the accessioning and stabilization workflow at this point. Digital materials are too fragile to sit on physical media carriers or in transfer data storage for long. There are too many ways they can be irrevocably altered or corrupted.

Notes

1. David Thomas, *The Silence of the Archive* (Chicago: Neal-Schuman, 2017).
2. The suggested deed of gift language was influenced by the Georgia Tech Library's deed of gift form.
3. "Exactly," AVP, https://www.weareavp.com/products/exactly/; "Data Accessioner," http://dataaccessioner.org/; "TeraCopy for Windows," Code Sector, https://www.codesector.com/teracopy.
4. Box home page, https://www.box.com/home.

Chapter 4

Accessioning and Stabilization Workflow

The accessioning workflow also includes what I refer to as the stabilization workflow (see figure 4.1). By stabilization, I mean that all the steps taken in this workflow make it so that the digital materials can survive in a state of benign neglect for as long as it takes your institution to move from accessioning to processing. However, benign neglect for digital materials is slightly different from what is done with paper-based materials. It requires that the digital materials be periodically audited and preservation storage be maintained.

The steps in this workflow could be individually done by human actors working with separate tools for each part of the workflow. At the opposite end of the spectrum, the workflow could be almost entirely automated, where the only necessary intervention from a human would be metadata creation and upload of data into a digital asset management system. Most institutions will fall somewhere between these two extremes. The guidance I provide in this section is meant to be high-level enough for you to adapt the strategies for your institution but practical enough for an institution just starting out to have a detailed enough road map to feel confident in moving forward building out its own workflows.

For each section of this and subsequent workflows, there are a variety of tools and services available to complete the steps. A community-built and -maintained directory of these tools, COPTR, is available for you to look through and determine the best possible avenue for your particular institution to take. There is also a more detailed and organized chart of these tools produced by POWRR.[1] However, this chart is a little out of date, so it could include tools that are no longer available, or the tools listed could have improved functionality that is not included in the discussion section of the chart.

Create Accession Record

The creation of an accession record is a process in and of itself, unique to each institution. There are commonalities in all the methods because the accession process is meant to capture intellectual and physical control over the materials acquired by your archives. The accessioning process starts with your donor engagement. All of the documentation that you generate while developing a relationship with the donor should be gathered together in a file.

My institution errs on the side of caution. Our practice is to gather the donor correspondence, the deed of gift, and printouts of any digital correspondence, which goes into an accession master file that is typically generated for the first accession in a collection. For those accessions that include digital materials, the accession master file should also include the donor survey or interview and any notes made by the archivist during a site visit. For additions to the collection that are separate accessions, either any documentation gets added to the original master file or a new accession master file is created. All of this documentation forms the legal evidence of custody, the written and signed agreements regarding what can and cannot be done with the materials, any restriction requirements, and the reference material that helps generate a description record later on in the processing workflow.

Beyond this accession master file, institutions typically maintain an accession database that contains an accession record for every set of materials acquired by the institution. This database could be a Microsoft Access or Microsoft Excel table, an ArchivesSpace instance, or a homegrown institutional web database.[2] In general, this piece of the accession record includes who donated the material, when it was donated, who

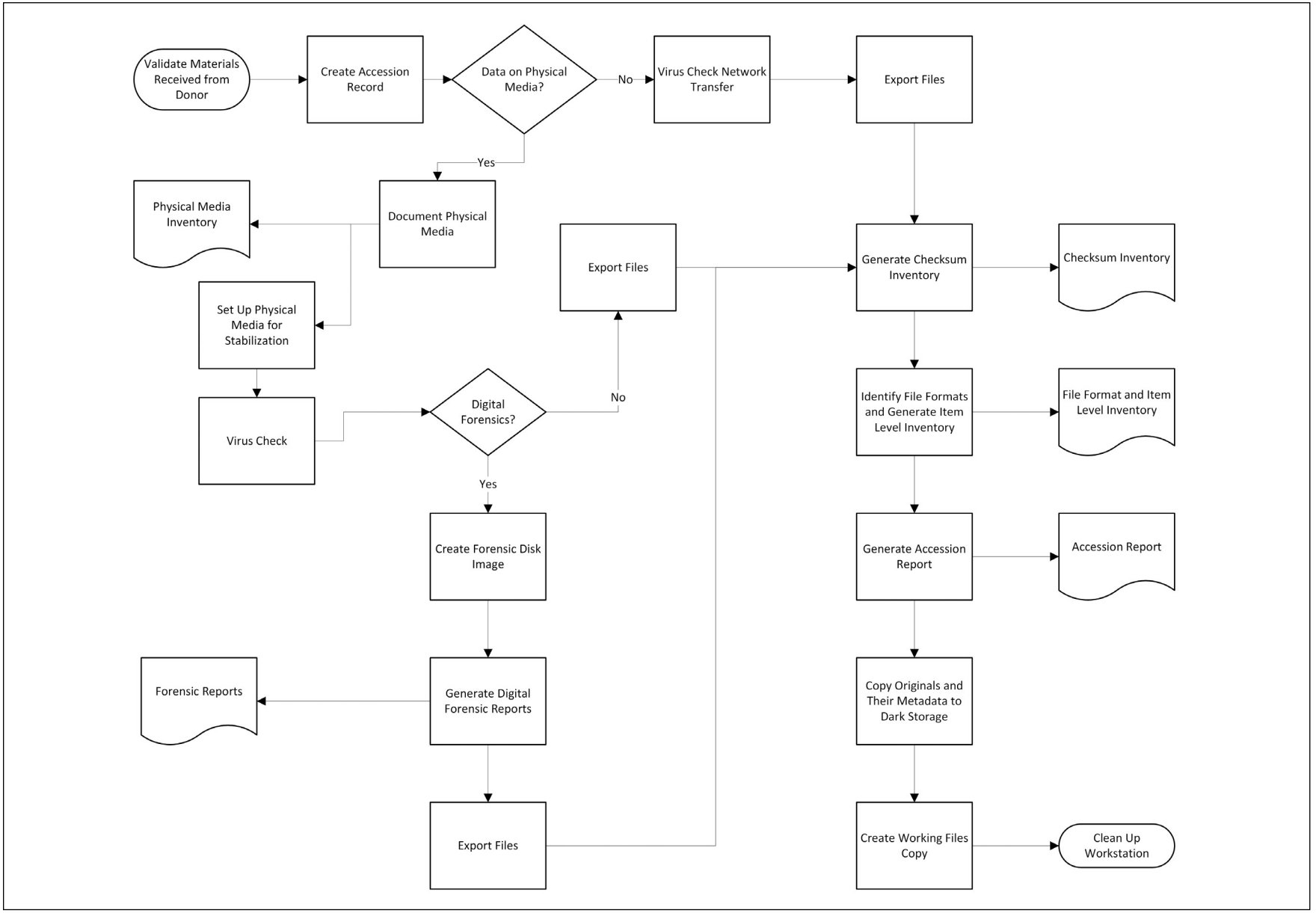

Figure 4.1
Diagram of a high-level accession and stabilization workflow

created the material, when it was created, approximately how much material was donated, and what kinds of materials were included in the donation. This information could be more detailed and broken out into subcategories depending on institutional processes, but the metadata generation process is typically the same regardless of what type of material is donated: paper, digital, or a mixture of the two.

Physical Media Pathway

Depending on how much involvement the archivist responsible for stabilizing the digital materials has with the donor, it may not be clear if an accession includes digital materials until the acquisition arrives at the archives. This is why an initial rough inventory is essential, preferably before the items are retrieved from the donor, but at the latest when materials arrive at the archives. Physical media carriers, such as hard drives and floppy disks, are much more sensitive to environmental changes and being dropped or jostled than paper records. I encourage you to separate these physical media carriers from their place among the analog records during this initial inventory. Depending on the circumstances, you may place a flag or separation sheet indicating that a floppy disk, CD, USB drive, or other physical media carrier was removed from a folder or box, but if there is no clear order to the materials, there may not be a need for such a flag or separation sheet.

Document Physical Media

When physical media carriers are part of an accession, try to make sure you have found all of the items before moving forward with the workflow. It is possible to add materials later, but some of the stabilization steps that are done at the very end of the workflow are meant to be done on the entirety of the accession at once. Once you have collected all the physical media carriers, give each media carrier an identifier. At my institution the identifier is very simple: the accession number underscore running item number. If there are fifty physical media carriers in an accession, the first would have the identifier AccessionNumber_001 and the last would have the identifier AccessionNumber_050. Other institutions include the type of physical media carrier as part of the identifier, for example, AccessionNumber_DVD_001. Optionally, this identifier can be directly written on the physical media carrier, or a sticky note with the number could be placed on the physical media carrier.

After an identifier has been assigned, you are now able to add the details about these carriers to an existing inventory for all the physical media carriers in the archive or create an inventory for the accession alone. Your institution's documentation workflows and systems will determine how you approach this task. The documentation for each physical media carrier and network transfer should include

- identifier
- accession number of the accession the materials belong to
- transfer type: network, physical media, e-mail, or digitized
- date the materials were acquired
- who the materials were received from
- who in the institution received the materials
- where the media is stored: physical location or server location
- media format: optical, flash, or magnetic
- media subtype: CD-R, DVD, USB flash drive, and so on
- manufacturer
- model number
- approximate age of the physical media carrier
- condition of the physical media carrier
- media label text (if any)
- if the media has been photographed

In some institutions, this inventory is also where the steps taken to stabilize and process the digital materials are documented. However, at the bare minimum, the items listed above should be recorded during the accessioning process. As you fill in the metadata for each physical media carrier, photograph the item, front and back, and include those photographs with the metadata for the accession so that you do not have to retrieve the physical media carrier for reference whenever you are working with the digital files for the accession. These photographs are also of interest to researchers because they provide researchers with a way to view how the creator organized and documented the physical media carriers without having to look at the actual items.

I want to make clear that the above documentation does not need to occur if you are retrieving digital materials from a donor using your own external hard drive or other temporary physical media storage device because that is just a transfer mechanism, not a permanent addition to the archive. Additionally, the above documentation will not need to occur if the donor expects you to return the physical media carrier. Again, the device is a method of transfer and not a permanent addition. However, all the subsequent steps for physical media will need to be performed.

Set Up Physical Media for Stabilization

First, gather any external hardware that you need to access the content on the physical media you are stabilizing. You will probably need to have on hand a

hub that allows you to access different types of flash media, such as SD cards, microSD cards, and proprietary digital camera memory cards. You will also likely need two or three different 3.5-inch floppy drives. Interestingly, even if there is no appreciable difference between floppy disks, sometimes switching between drives will increase the likelihood that you can access the content on the floppies. There is also a possibility that you will need to acquire a system to access 5.25-inch floppy disks and Zip disks. These are the most common materials I have found at the different institutions I have worked at. After setting up the external hardware to access the media items, you will need to set up your write blocker.

Anytime a computer's operating system interacts with physical media carriers, there is the potential for the technical metadata attached to each digital file in that physical media carrier to be inadvertently altered. To prevent this, physical media needs an additional safeguard of a write blocker setup before media is connected to your digital materials processing station. As an aside, I encourage you, if you have the resources, to have a standalone station dedicated to the stabilization of digital materials. This is a major safeguard against viruses that not only protects the unstabilized physical media and newly transferred digital materials, but also protects those materials already in your preservation system.

A write blocker can be a physical device or a piece of software that is turned on and off as needed. My institution uses a combination of both. The software is depended upon only if the hardware write blocker is incapable of interacting with the physical media. This often occurs with physical media older than a 3.5-inch floppy disk. After the write blocker has been set up, you now need to choose if you will be doing digital forensics or simply making a logical copy of the files on the physical media device. I mention digital forensics solely in the physical media section because many of the software tools used by archivists that perform digital forensic analyses require disk images, which are most commonly acquired from physical media items.

Virus Scan

Before doing anything, check the materials for viruses. I am using the term virus to cover any malicious programming that could be found on materials you are bringing into the archive. Most computers now come with built-in security that includes the ability to scan discrete sections of files for viruses and even allow for the quarantine of affected files. Generally, when viruses are found, you will need to involve your information technology department to determine if the virus can be dealt with or if you should deaccession the affected material. There are open source virus resolution solutions available, one of which is integrated in the BitCurator suite of software. However, it may be that the information technology department in your institution has a workflow regarding virus checking and remediation that it would prefer you to follow, so be in constant communication with your information technology experts.[3]

Forensic Disk Image

If you have decided that a physical media item warrants digital forensic analysis and you have the donor's informed consent to perform this analysis, you may then proceed with this section of the workflow. Using the digital forensic software suite of your choice—BitCurator, KryoFlux, Forensic Toolkit (FTK), or some other tool—create a forensic disk image for each physical media item.[4] This is a bit-for-bit copy of the physical media including empty space. Part of the creation process will include embedding metadata about who is creating the disk image, the identifier the disk image is associated with, and so on, into the disk image file. After you have created the disk image, you will then export the digital files from the disk image and export the technical metadata associated with the disk image, specifically the file system metadata that includes how a computer was used by the creator, deleted files that have not yet been overwritten by the operating system, and more. Be careful to make sure that all the metadata files are named in such a way that they remain associated with the disk image file. This is most easily done by using the physical media identifier as part of the file and folder names.

Logical Copy

If you have decided that in-depth digital forensics is not warranted, there are several methods you can use to make a logical copy of the files on the physical media devices you are using. If you have a digital asset management system, homegrown or subscription service, you will most likely be using the tools built into that system to copy the files directly into the system. If your protocols require the transfer of files to a local machine before they are moved into the digital asset management system or if you do not currently have a digital asset management system, you need to use a piece of software that will perform multiple functions at once. Ideally the software will copy over files without changing the internal file metadata such as creation date or creator, will generate a report containing the technical metadata for each file, and will verify that the files were transferred without any loss or change to the data of each file. I use DataAccessioner for this, but there are other options.

Network Transfer Pathway

By network transfer, I mean any receipt of materials not on a physical media carrier, so this could include e-mail, materials donated through a web form, those placed in a cloud storage service for you to download, or an actual network transfer using file transfer protocols. When possible, communicate and test out the transfer methodology you and the donor have agreed to. The tests will help reduce the chance of technical problems due to hardware or software incompatibilities, and the donor will feel more confident in using the method to transfer materials to your institution. This confidence is especially important if you expect that the process will need to include multiple transfers. The best-case scenario for a network transfer is to use a tool that will package the data and will verify that the package was unchanged after the transfer is complete, such as Exactly.[5] The packages can then be sent via any method that works well for you and the donor.

Stabilize Accession

After you have transferred all the materials for an accession to your working space, it is time to perform the stabilization process. This is accomplished by generating technical and administrative documentation for the entirety of the accession, not just the discrete parts. Then move the accession as a whole into your preservation storage system.

Generate Technical Metadata

While you may have generated technical metadata, such as file creation date, file format type, or a checksum, using discrete tools for the individual pieces of the accession, it is a good idea to generate one single listing of all of this information for the accession as whole. This allows you to have all the information in one place and also doubles as a file-level inventory of the materials, including their current location in the overall directory for the entire accession. This one document is essential to later appraisal, preservation, and arrangement and description work. Even though it seems like repeating steps you have already completed, it is really worth doing. The tool we use at the University of Montana for this is DROID.[6]

Generate Reports

The final documentation step here is to generate some kind of accession report. This report is meant to be a brief overview of the entire accession and will be used later when you are processing the collection. The accession report is also a way to quickly remind yourself of what is in the accession. This could include any potential preservation issues that may need to be remediated in the future, such as unique file types that require specialized software to access or older file formats that will need to be normalized into a standard preservation or access format. Our accession report asks the archivist to document the following:

- Overview
  - accession number
  - deposit date
  - transfer type
  - collection number (if known)
  - creator
- Physical details
  - number of media
  - extent/data size
  - number of files
  - file format types
  - preservation issues
  - preservation recommendations
- Intellectual details
  - current organization
  - date range
  - content summary
  - privacy issues
  - donor restrictions
- Report author
- Report date

Move Accession to Storage

After all the data has been transferred, stabilized, and documented, you can now transfer the accession to your preservation storage environment. My recommendation is to transfer the digital materials into two separate locations. One set will go to preservation storage, and one set will go into working files storage. The preservation storage set should be the unaltered originals in your "dark archive," the place that very few people have access to and is accessed only to remediate cases of accidental or deliberate corruption of your working files copy. The working files are what you will process. These will eventually become the files your end users have access to. At this point, your materials can wait however long is needed until you are ready to process them.

Notes

1. "Community Owned Digital Preservation Tool Registry (COPTR)," main page, last modified June 4, 2020, http://coptr.digipres.org/Main_Page; "Tool Grid," Digital POWRR: Digital Preservation Research, https://digitalpowrr.niu.edu/digital-preservation-101/tool-grid/.
2. ArchivesSpace home page, https://archivesspace.org/.

3. BitCurator home page, http://bitcurator.net/.
4. BitCurator; KryoFlux home page, https://www.kryoflux.com/; "Forensic Toolkit (FTK)," AccessData, https://accessdata.com/products-services/forensic-toolkit-ftk.
5. "Exactly," AVP, https://www.weareavp.com/products/exactly/.
6. "DROID (Digital Record and Object Identification)," GitHub, https://digital-preservation.github.io/droid/.

Chapter 5

Processing Workflow

This workflow (see figure 5.1) is where the majority of archival silences and institutional biases can be brought to light and overcome. As the person responsible for appraising, arranging, and describing these materials, you are responsible for being aware of your personal biases and the perspective you are bringing to the processing of the collection. Involve the creator of the materials, the donor, and the community of origin as much as is possible through direct communication. Have them review the arrangement and description so that unintentional misrepresentations and misunderstandings do not occur due to archivist-created content. Share this power with the creator and community so that the historical record is as inclusive as possible.[1]

Depending on your institutional context, a different team may be processing the collection than those that did the original acquisitioning and accessioning. That is why the documentation generated during those workflows is particularly important. That documentation includes critical contextual clues for processors to follow when they are doing their appraisal and developing their arrangements and descriptions. In most cases, collections that contain digital materials are a hybrid of paper and digital materials. However, as time goes on, we will move toward a situation where most collections will be digital only and the rarities will by hybrid or paper-only collections. Currently, it is rare to have only digital materials, and when this does happen, it is quite often a digitized collection—that is, a digital version of a physical collection created by scanning the original physical materials. In some institutions, digitized collections do not go through the digital preservation workflows because the institution holds the paper originals and considers those originals as the preservation priority. I have found, though, that there are instances where the digitized version is all that you have, or where so much effort and financial resources went into a digitization process that it is a risk management decision to include these files in the digital preservation program.

Hybrid Collection Peculiarities

Hybrid collections that have resided in your institution long enough very likely have already had the physical pieces of the collection processed, including a published description, and are available for researchers to access. In these cases, there may have been no available workflow for processing the digital parts of the collection so there is only a note in the description mentioning that these files exist but are currently inaccessible. In the case where the physical content is already processed, the main decision to make is whether to integrate the digital files into the existing arrangement and description or whether you need a completely new series solely for the digital files. However, if no part of the collection has been processed, you will have the option of creating a plan for the entire collection as a whole, from the beginning.

That being said, in my experience, it is far easier to assess the physical materials and create a processing plan based on the intellectual contents of those materials before ever touching the electronic files. There are some simple reasons for this. The first is that it is much easier and quicker to skim and flick through pieces of paper than it is to access a series of discrete digital files. With paper, all you have to do is turn the page. With digital materials, you have to wait for the software to load the information. No matter how advanced your current computer, there is always a time lag when moving between digital files. Also, paper materials are much easier to lay out and rearrange than digital files. Again, with paper all you have to do is pick it up and move it. With digital files you must copy or move the files and then verify that

the files have not been affected during the process. The larger the file you have to copy or move, the longer the transfer and verification process takes. If you have a general idea of the organization and content of files from the physical records, you will have a much easier time appraising and organizing the digital files.

Develop Processing Plan

A processing plan could be a formal document that describes the steps you will take in appraising, arranging, and describing the materials with a time line for when each step should be complete. Alternatively, your

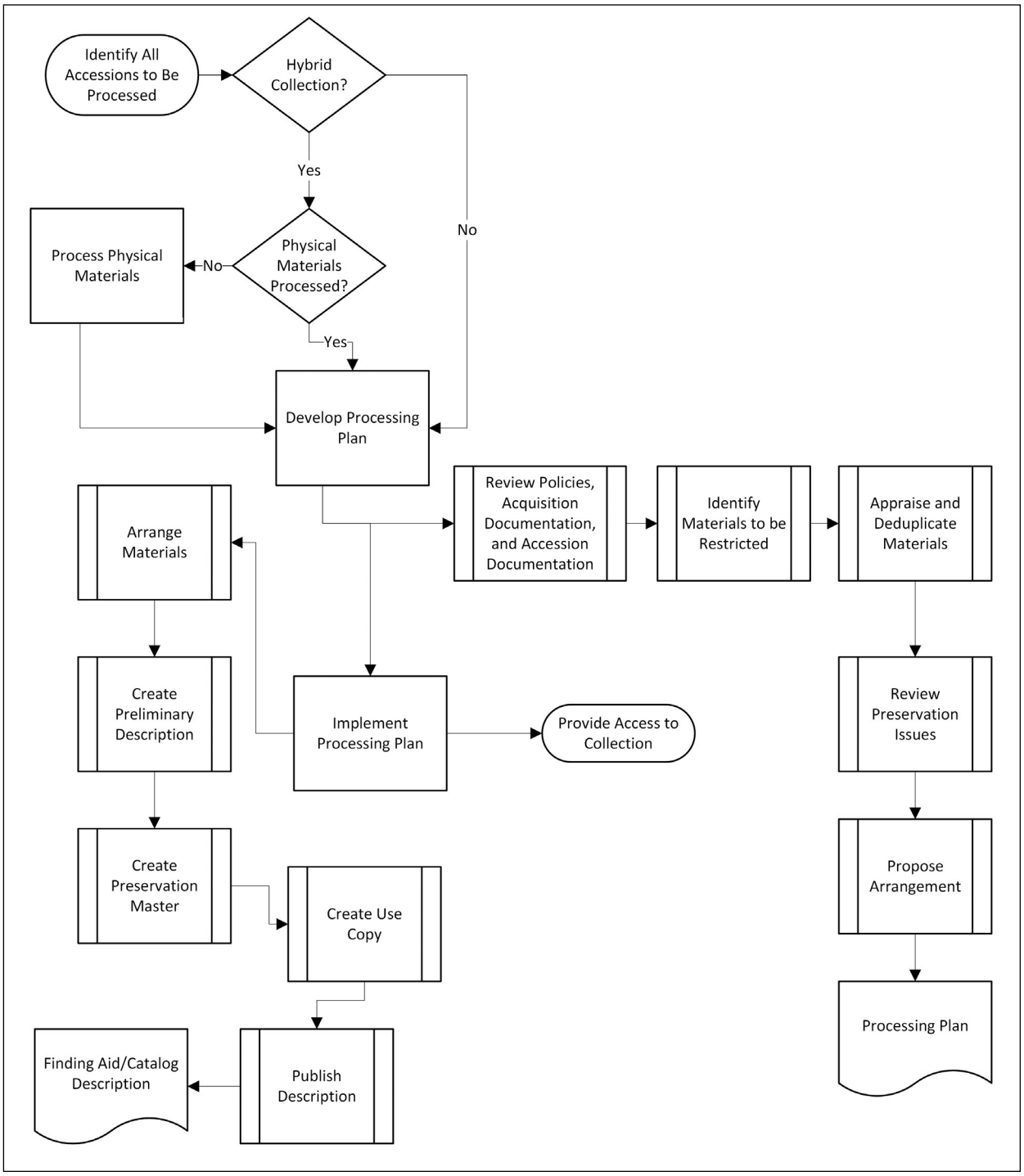

Figure 5.1
Diagram of a high-level processing workflow

processing plan could be an informal set of notes and outlines. This is again dependent on your institutional context. However formal the process, there should be documentation of the decisions you make at each stage and why those decisions were made. This documentation is evidence of the steps you took to make the collection available to researchers and is part of the institutional memory that makes your decisions and justifications transparent to any future archivist.

Review Policies and Donor/Creator Documentation

Before opening a storage box or a digital file, go to the master files for all the accessions that make up the collection. Review the deeds of gift, donor surveys, donor interviews, and any communications with the donor that document your legal obligations in regard to restrictions and what to do with discarded materials, as well as giving a contextual overview of the materials in the collection. Make notes on what to be aware of and where potential private information may be.

Identify Materials to Be Restricted

Using the donor-provided documentation about what materials need to be restricted and where those materials currently live in the collection, if provided, and a standalone tool like Bulk Extractor or the built-in functionality of your digital asset management system, review the flagged materials for potential restriction.[2] Generally, the software tools will flag only personally identifiable information for you to review, items like social security numbers, credit card numbers, phone numbers, and addresses—text that follows a pattern and can be used to steal someone's identity. If the person linked to any of this information is deceased, you often do not have to restrict any of it. Alternatively, if the person is still alive, the individual files that contain this information need to be restricted, redacted, or removed from the collection. For other types of personal information that the donor wants restricted, you are dependent on the donor to give you a map to where this information may be in the collection or distinct keywords to search for in the files to help you find it.

After identifying restricted materials, you have two options. You can immediately remove the material from where it is currently located in the collection and move it to a separate digital folder for restricted material for the entire collection. The second option is to continue with the workflow until you have a proposed arrangement and then restrict the materials in a separate folder that is intellectually associated with where the material belongs in the arrangement. That intellectual association is generally done through the folder name.

Appraise and Deduplicate Materials

If you have a digital asset management system, you will be appraising the files within the system, and the system will automatically remove duplicate files based on the parameters you set when implementing the system. However, if you do not have a digital asset management system that includes processing functionality, there are tools such as TreeSize or WinDirStat that generate a visual overview of the collection and a detailed listing of the types of content included.[3] The visualization breaks the collection out into content types such as video files, audio files, word processing files, and so on. The tools also provide an analysis of how much data and how many files are in the collection, which are key pieces of information for your final description and for determining the best avenues of eventual end user access.

These tools are invaluable during the appraisal process, and some can do double duty of analysis and deduplication. I use TreeSize Professional for this very reason: it allows me to appraise the materials and deduplicate the files in the same step. Using the bird's-eye view of the collection and the more detailed hierarchical view provided by these tools will allow you to determine most of your arrangement without having to review individual digital files. For institutional records, these tools also help you quickly determine if there are personal files that were inadvertently donated alongside the institutional records that were transferred.

Review Preservation Issues

For those institutions that do not have a digital asset management system that will automatically normalize files into standard preservation formats upon transfer into the system, there are several documents created in previous workflows that can help you determine if there are potential preservation issues in the collection. These include the donor survey, the accession report, the more detailed technical documentation generated during the accessioning process, and the collection analysis done in the previous appraisal step. Using all of this information, determine if there are any files your institution does not have the resources to provide end user access to. Document what these files are and determine if they are worth keeping or if they are to be deaccessioned. Be sure to include these decisions in your final description of the collection.

Propose Arrangement

After reviewing all the documentation and the files themselves and making deaccessioning decisions, outline your proposed arrangement. The first decision to make for any type of collection is if you will actually be rearranging the files. For digital-only

collections where the creator-imposed organization is clear enough for users to follow, all you have to do is describe this arrangement in the finding aid. It may also be the case that the collection is so large, regardless of existing organization or lack thereof, that no rearrangement of files is feasible. In this instance, that is what is documented in the finding aid, along with any additional information that can be provided from the initial appraisal steps. For digital-only collections where you are imposing an arrangement, outline the proposed arrangement as you would in a finding aid. Have another archivist review the arrangement, if possible, to see if it makes sense to someone not embedded in the collection, just as you would have a friend review a draft of your journal article before turning it in to a publisher.

For hybrid collections where the physical portion of the collection is already processed, you will need to decide if the digital files will fit well within the existing arrangement or if you need to propose a standalone series for the digital files where you can outline an arrangement that better fits the current organization of the digital material or simply describe the creator's organization of their files. For hybrid collections where you are simultaneously processing the physical and digital materials, you will need to determine an arrangement that best fits both sets of materials. Again, you could decide that it would be best to separate out the digital files into their own series, but it is less likely that this will be the case because you are not having to deal with legacy processing decisions.

Implement Processing Plan

Arrange Materials

You should follow your institution's processing workflow for implementing your arrangement on the physical materials. If you have decided to impose a new arrangement on your digital materials, I suggest creating the new folder hierarchy in a staging location first and then moving the digital materials into the folders. That way you can start and stop the process as needed, and you are less likely to accidently delete files or alternatively copy files into multiple unintended locations. Also, if your institution does not have a digital asset management system that will automatically sanitize filenames (remove special characters) or normalize the file formats into a standard preservation format, you will need to do this as you transfer materials into their final arrangement. If you have a digital asset management system, those steps are most often taken care of when the files are transferred into the system.

The implementation process I use is as follows:

- Move files into a folder structure that mirrors the layout of the finding aid, using file transfer software that verifies the files were not changed during the move, such as TeraCopy.[4] For example:
  - Mss###_CollectionTitle
    - Series_I_Personal
      - Subseries_1_Finances
        - Put all the files and folders that belong in the Finances subseries into this folder.
- If there are restricted materials as part of the collection, create a "RESTRICTED_ Mss###_CollectionTitle" folder hierarchy that mirrors the finding aid. Have that folder hierarchy's access limited by username to the head of the archives, the digital archivist, and the processing archivist.
- If there are files to be normalized, save the new versions of the file into the destination folder instead of moving the original file.
- Using a file renaming protocol, such as ReNamer, sanitize filenames in the folder.[5]

After the files have been arranged, delete your working files copy so there is no confusion over what version of the collection to carry forward into the rest of the workflows.

Create Preliminary Description for Materials

After you have arranged the materials, draft the finding aid text relating to the digital materials. There are guidelines for this in *Describing Archives: A Content Standard (DACS)*.[6] Part of creating this draft will be deciding if you will include direct links from the finding aid to the digital materials or if users will have to request access. It is not an all-or-nothing decision. It could be that there are direct links to some of the materials in the collection, while other require mediated access. Have at least one other person review the description, preferably someone who was not involved in the processing of the collection, for readability and usability. Ideally, the donor or creator would also be able to review the draft description before it is published. If that is not possible, I would recommend that part of the engagement with the donor include an emphasis on the fact that they have the ability to request that changes be made to the description as needed.

Create Preservation Master

After you are completely satisfied with your arrangement, create a preservation master of the complete collection. This could be done automatically through your digital asset management system. Alternatively, this could be the point where you transfer the materials to a system such as Archivematica.[7] I have found this system works best on a fully arranged collection; it will automate the process of creating a preservation

master copy and a use copy. Your preservation master could simply be a copy of the fully arranged files placed in your dark archive with their administrative and technical metadata generated during accessioning and stabilization.

Create Use Copy

With the preservation master carefully tucked away, you are now ready to create your use copy. The use copy of the collection is what you provide to your researchers. The major difference between the preservation master and the use copy is for content such as videos, audio files, and images. The file types will be different, and the file sizes will be smaller. For example, the preservation master of an audio file could be a WAV at close to a 500 megabytes. The use copy of that same audio file would be an MP3 at close to 160 megabytes. Generally, if you do not have a system to automate the creation of use copies, you would focus on creating use copies only of very large files that would be difficult for users to access over the web because the bandwidth needed to stream or download them is beyond what most researchers at home reliably have access to.

Integrate Description into Finding Aid/Catalog Description

Only after you have created the use copy for the collection should you create or modify the finding aid. In this way, if you are creating direct links from the finding aid to the digital materials, you will have to do so only once. This is incredibly important if you are hand coding your finding aid versus using a tool such as ArchivesSpace.[8] Either way, having drafted your description already, it should be a matter of copying that draft into the tool you use to generate finding aids for the final published document.

Notes

1. Archives for Black Lives home page, https://archivesforblacklives.wordpress.com/.
2. Simson Garfinkel, "bulk_extractor," GitHub, https://github.com/simsong/bulk_extractor.
3. "TreeSize," JAM Software, https://www.jam-software.com/treesize/; WinDirStat home page, last updated November 12, 2018, https://windirstat.net/.
4. "TeraCopy for Windows," Code Sector, https://www.codesector.com/teracopy.
5. "ReNamer," den4b, https://www.den4b.com/products/renamer.
6. Society of American Archivists, Describing Archives: A Content Standard (DACS) (Chicago: Society of American Archivists, 2004, 2013), https://www2.archivists.org/groups/technical-subcommittee-on-describing-archives-a-content-standard-dacs/describing-archives-a-content-standard-dacs-second-.
7. Archivematica homepage, https://www.archivematica.org/en/.
8. ArchivesSpace home page, https://archivesspace.org/.

Chapter 6

Access Workflow

As with all other aspects of archiving and librarianship, the answer to how users gain access to digital materials will always be "It depends." It depends on institutional policy, on the resources the institution has to provide equitable online access to materials, on whether the institution has the ability to provide mediated access to materials that require special software to access, and many more variables that determine how and when a user can access digital materials.

The access workflow (see figure 6.1) shows two clearly defined pathways for providing access to digital materials: direct access and mediated access. In direct access, users are able to find and view digital materials without any need to contact the institution of origin. Mediated access *requires* the user to contact the institution to gain access to materials, either because the materials are not available online or because the user needs credentials to access the materials that are available online. Your institution's policies will determine if direct access to born-digital materials is viable or if only digitized materials will be made directly available to users.

There is also the question of whether users will be able to gain access to unprocessed materials. There is a clear precedent for this with physical materials, especially if institution members wish to gain access to institution-produced content or a creator's family members wish to access materials by or about themselves. Therefore, you must be prepared for users to ask about digital materials mentioned in finding aids that are not yet processed or to request access to unprocessed materials that users know to be at the archives but are not yet part of an existing collection. Realistically, due to privacy concerns and the exponentially larger volume of digital material compared to physical material, an archivist may need to review materials before providing a user access to unprocessed digital content. A risk-averse institution will simply restrict digital materials until they are processed. However, for low-risk collections, where all the accession documentation clearly indicates there should be no privacy problems and the materials are fairly easy to review using file viewer and analysis tools, it will not always be an automatic no.

Unprocessed Materials

If you do not currently have a policy regarding user access to unprocessed materials, start there. The policy will support archivists who interact with users requesting access, will create transparency about who has access to materials and why, and will clearly delineate who is responsible for making the decisions on a case-by-case basis. Your policy may very well state that no access to unprocessed digital collections material will be allowed. As long as that policy is consistently applied to *all* users, there should be no problems with implementing it. If the policy allows access to some unprocessed materials, you must very carefully delineate the terms of that access and how those decisions will be made and then consistently apply that policy.

Access to unprocessed material, digital or physical, is always mediated by an archivist in some way. Typically, the user does not gain access to the entirety of the unprocessed materials (unless the accession is very small). Instead, the user clearly states their research question and what they are hoping to find within the unprocessed materials. An archivist then uses the guidelines to carefully extract a subset of the materials and provides them to the user. I would suggest, when providing these materials to users, it not be through e-mail. Instead, access should be through more secure means, such as requiring a user to come to the archives and access the materials via a reading room computer or through a cloud storage environment that requires some form of authentication to access.

After consulting your policy to determine if access to an unprocessed accession is warranted, you must then determine how much of the accession to provide the researcher. Is it a fairly small accession that would be easy to remove any restricted material from? Or is it a large collection that would take more time than is feasible to sort through? For a large collection, I suggest having the researcher be as specific as possible about what content they are looking for, including specific keywords for you to use when examining the

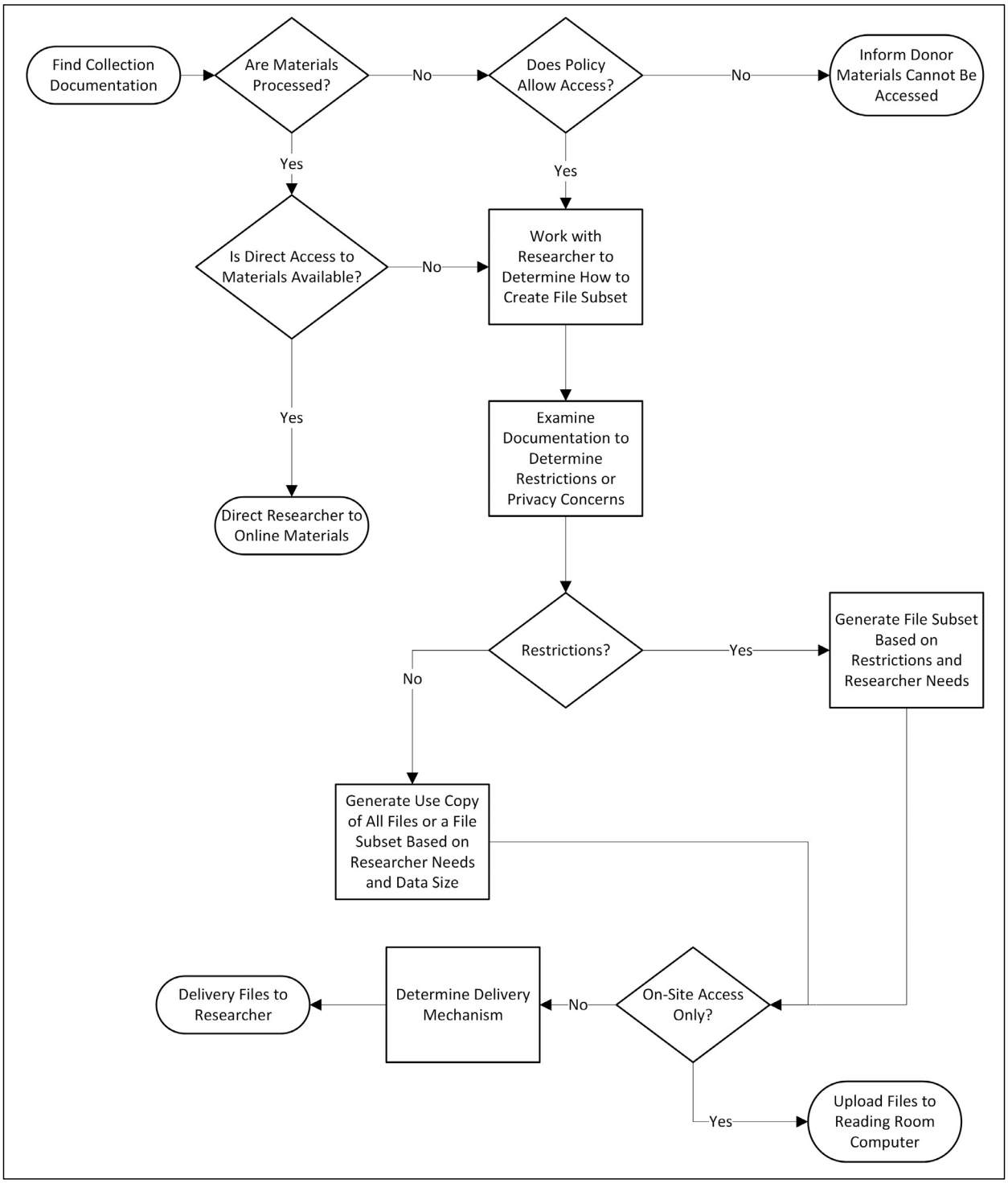

Figure 6.1
Diagram of a high-level access workflow

accession. Then, you can use either your computer's built-in file explorer or a tool like TreeSize to search for items in the accession that might be useful to your researcher.[1] Whether you are providing the entire accession, minus restricted material, or a small subset of files, you will need to create a staging location to copy files into for the researcher before moving on. By having a staging location, you will prevent potential accidental alterations to your working files copy.

Then you need to determine if there are materials in the accession that are restricted or at least too sensitive to grant researcher access to at this time. For this, I use a three-step process. First, I examine the accession master file to determine if there are any materials the donor has specifically requested be restricted and to see if there is the potential for personally identifiable information in the accession. With those guidelines in mind, I use a tool such as Bulk Extractor to search for personally identifiable information if this process has not already been completed in a previous workflow.[2] Finally, I remove any restricted material from the staging set of files.

Now that you have a file set ready to deliver to the researcher, you must determine how you will do so. Typically, there are two options for unprocessed material, reading room–only access or providing the files through a cloud storage service that requires the researcher to go through an authentication process before accessing the materials. The reading room option is the most restrictive and security-conscious. It requires the researcher to come to the institution and use the reading room computer to access the files. In some cases, these reading room computers have been specially modified so that the external ports that allow flash memory devices to be inserted have been deactivated, access to the internet and internal institutional networks has been removed, and other security measures have been put in place so that the researcher has access only to the materials that have been preloaded on the machine with no ability to download or remove those materials from the machine. In other cases, the machine has not been altered and the researcher is on their honor to follow the rules set by the archives regarding copying of the materials that have been preloaded on the machine.

The second option is to provide the materials to your researcher through a cloud storage service provider such as Google Drive, Box, Microsoft OneDrive, and so many more. This option does not require a researcher to come to the institution, which allows you to provide this service to a much more geographically diverse set of researchers, and if a researcher has accessibility needs, they can use their own computer setup where the tools they need are available. All of these services allow you to set limits on what researchers can do with the materials, so depending on your policies, the researcher may have only view access, or they may be able to download the items. Also, these services allow you to automate when permissions are rescinded so that the researcher does not have perpetual access to the materials. Finally, the sharing mechanisms on these services almost always automatically include authentication steps. This is due to the ways access to shared material is linked to specific e-mail accounts or user accounts so that access given to a researcher would not be able to be shared beyond that person.

Processed Materials

For processed materials, the mediated pathways described above are also an option, albeit often with fewer restrictions on researcher behavior. However, there are also multiple unmediated ways for users to access materials. Examples include clicking on a link in a finding aid, searching through an institutional repository, landing on the public interface of a digital asset management system, or accessing items through your institution's online library catalog. The key difference between mediated and unmediated access is that, for unmediated access, while an archivist, librarian, or curator may have helped researchers find the material, the intervention of these professionals is not required for researchers to gain access to the material.

Often the decision about whether materials will be available through unmediated access occurs during processing because the mechanisms to provide that kind of access generally need to be built into the final description of the materials. When these decisions are made after processing has been completed, you need to modify any existing descriptions to point to the access location in some way, either through building collection-, folder-, or item-level links to the access location, by adding text to a notes field about how to access the materials, or by building out the description in the digital asset management system's public user interface. During or after processing, the workflow for building out these descriptions will be dictated by your institution's policies on description and existing workflows regarding the tools used to create those descriptions, be it encoding the Encoded Archival Description or using a tool like ArchivesSpace to create a resource record that will eventually become the finding aid.[3]

Notes

1. "TreeSize," JAM Software, https://www.jam-software.com/treesize/.
2. Simson Garfinkel, "bulk_extractor," GitHub, https://github.com/simsong/bulk_extractor.
3. ArchivesSpace home page, https://archivesspace.org/.

Chapter 7

Maintaining Digital Materials over Time

This chapter is slightly different from the others because if you have created and consistently implemented workflows for all the other stages of the digital material life cycle, most of the work for ongoing maintenance has been done. When I mention the digital material life cycle, I am referencing the general iterative process of create, acquire, stabilize, appraise, process, and provide access to that I discussed in previous chapters. These actions are all part of the digital preservation process. There is a formalized reference model available from the Digital Curation Centre called the Curation Lifecycle Model, which provides a more comprehensive view of the preservation of digital material, specifically data, from conceptualization through final disposition, where disposition may mean remaining in the preservation cycle or permanent deletion.[1]

In an ideal world, the maintenance of digital materials is automated and your responsibility is to periodically review the system and make upgrades and tweaks as needed to keep the machine running smoothly. In fact, in many institutions this is the current reality, but for others it is an unrealized ideal. In an acknowledgement of this spectrum of resources and abilities, I have structured this chapter based on three of the five functional areas found in the National Digital Stewardship Alliance's (NDSA) "Levels of Digital Preservation."[2] The final two functional areas, content and metadata, have been thoroughly covered in the accession and processing workflows.

The "Levels of Digital Preservation" document was created to be as adaptable as possible to the many different types and sizes of institutions that currently and will in the future curate digital materials. This document focuses on the technological aspects of digital preservation; however, technology is not the only key to maintaining your digital materials. You must also constantly keep your organizational infrastructure and resource allocation at levels consistent with the amount of material you are preserving. The chapter will conclude with discussions on how to maintain both. Depending on your own institutional context, each of these sections may have a lower or higher priority determined by policies, currently allocated resources, and risk assessments. For every one of these sections, documentation is key. It is essential to keep up-to-date records of every aspect of your program in a central location for anyone who is working with digital materials to access. This documentation acts as reference material, advocacy and outreach material, and an audit trail of all you have done to increase the transparency of your actions and policies.

Storage

There are some standard requirements in regard to storage of digital content. Beyond those basic requirements, how robust and diverse your storage is will depend on your institution's resources. If your digital preservation program is entirely standalone, you will make all these decisions. However, most digital preservation efforts are integrated into a wider ecosystem where storage is mostly dictated by the information technology department of your institution. Where that is the case, you will need to have an open line of communication with the information technology staff to come to an understanding of current practice and negotiate possible changes to make the storage of digital materials more robust, as needed. Keep the relationship strong and the conversations on a schedule so you are not caught unaware by any changes or updates to your institution's storage strategy. Also, these conversations should encourage the information technology department to take ownership of its part in the digital preservation program. The more invested it is in the success of the digital preservation program, the stronger a partner it will be.

As a community, digital preservation practitioners encourage that there be at least three complete copies

of all of your digital content. The bare minimum is two copies. Furthermore, these copies must be on separate storage mediums. For example, if you have one complete copy on a computer or your library's server system, the other copy should be on a completely separate type of hardware or in a cloud storage environment. The hardware diversity helps prevent a single point of hardware failure causing data loss. In addition to the number of copies and diversity of storage type, standard practice is to have at least one complete copy of your digital materials in a completely separate geographic location. This could mean having a copy of your backup tapes in a partner institution in at least a different state. Another option is having your cloud storage copy be in a different geographic region than your home institution. The geographic diversity is meant to spread the risk of a single natural or man-made disaster decimating all of your data in one event.

As with all technology, your storage devices will age, so keep a schedule of when you purchased storage, that device's approximate lifetime, and the budget for its replacement. In the case of cloud storage, budget for your subscription every year and leave yourself a little room in the budget for an unexpected increase in needed storage capacity. In some cases, pulling a copy of your materials down from cloud storage incurs a cost, so be prepared for that. Common reasons for needing to retrieve data from the cloud include a local hardware failure that requires you to replace all of your local copies of your data, switching cloud storage services, or needing to retrieve only small amounts of data due to the local copies being irrevocably damaged due to an accident or an act of malfeasance.

Document all current storage mediums, their physical locations, and the backup schedule. Keep track of how much data you have stored and be aware when you are about to reach the limits of your current storage capacity. Careful documentation will help you plan for gradual increases in storage capacity and slowly build the necessary increases into your operating budget. However, there may come a time when an accession could exponentially exceed your current storage capacity. If this were to occur, there are three avenues open to you: requesting the donor to provide financially for the storage of the material, advocating for additional storage resources on an expedited time line, or making the difficult decision to recommend another institution for the donor to work with.

Integrity

This section focuses on maintaining the integrity of the digital materials in your custody. In this context, integrity is ensuring that you can prove that the digital content received from the original creator is the same content that a researcher eventually has access to. This is much easier to do with physical materials such as papers and books than it is with digital content due to the very nature of digital material. Digital content is meant to be copied, shared, and modified easily, so maintaining a static version of the materials requires establishing the state of the material when it arrives in your institution and then maintaining that state throughout the life of the digital material while it is under your care.

If you have established an accessioning and stabilization workflow, the first part of this has been done. You have checked all incoming material for viruses and documented the thumbprint of each file by recording the materials' checksums. As part of your digital preservation maintenance workflow, you will periodically regenerate checksums and compare them to ensure no changes have been made to the material. If an undocumented change has been made, delete the local copy and pull down a new version from your preservation masters. Many digital asset management systems automate this process and create an audit log that you can monitor. However, if you do not have one of these systems, there are several tools available, one of which is Fixity, that you can use to at least automate the checksum comparison on a schedule and that will provide you with a report after every pass that you can use to determine if further action needs to be taken.[3] The audit logs of these comparisons are just as critical as the performance of the comparisons themselves because the audit logs provide transparency about the state of your materials and any changes made to them.

There will be instances where you will deliberately change the nature, format, or content of the material in your care. This will cause a change in the checksum and throw a flag during the integrity checking process. Again, thorough documentation of all actions taken during processing will help explain the flags raised during the first round of integrity checks after the changes have been completed. Part of guaranteeing integrity is doing these checksum comparisons after every transfer of materials and keeping the audit logs of the integrity checks in a secure location.

Control

This section is all about security, who has access to content, who is authorized to modify and delete content, and how you keep track of those permissions. The single greatest enemy of digital material, besides time, is human interaction. The most common reason, at my institution, that we have had to depend upon backups of our digital content was accidental modification by a user. It is imperative that your institution

have a strong permissions structure that automatically denies unauthorized users access to content.

System administrators, usually housed in the information technology department for local network systems, are responsible for setting these permissions, but this not an automatic process. To be able to set these permissions, system administrators need to know who, what, and how—who has access, to what content, and how far that access extends. This information is most easily communicated in a table where you list each user, what they have permission to, and how far that permission extends (see table 7.1). Annually, at the very least, this table should be reviewed and permissions changed as needed. Also, after an event such as a staff member leaving or a new person being hired, this table should be updated and immediately communicated to the system administrators. This security plan works just as well for digital asset management systems and other tools and services you use to carry out digital preservation workflows, so be clear what each table is for and keep each document up to date.

Organizational Infrastructure

Digital preservation relies on a stable budget of financial resources and personnel time. Organizational infrastructure plays a vital role in maintaining that stability. From the top administrator down to the newest employee, knowing who is in your organization, what their responsibilities are, and what their priorities are will help you to successfully advocate for your digital preservation program and find willing partners in performing your responsibilities.

Another vital tool in your knowledge bank is a thorough understanding of the policies and procedures that guide your institution. Those policies will determine who you should approach for help on specific projects and when to advocate for more resources in the cycle of fiscal allocations. For example, your institution may require that all software be managed by the information technology department. In this scenario, any time you want to test or implement a new piece of software, you must get approval from your information technology department and work with it to have the software downloaded on your personal work machine. This even includes software that is open source and therefore does not require financial resources. Building and maintaining a strong relationship with your information technology department personnel will make this process much less frustrating.

Let us consider another scenario, one where all purchases must be requested and approved through a specified process before the end of the fiscal year. In this situation, you need to be aware not only of the structure of your institution's fiscal year—for example, July 1 to June 30 or January 1 to December 31—but also the rhythm of that fiscal year. Historically, has there been a purchasing freeze at least a month before the fiscal year ends? On average, how long does it take requests to work through the process? Are certain types of requests more likely to be approved than others? All of this information will help you format your requests and craft the most successful argument for your request and the ideal time in which to place it.

In the final scenario, I would like to address changing organizational infrastructure. It is the nature of any institution that people will come and go and leadership priorities will change. You need to build out your digital preservation program and all of its workflows to be sustainable amid change. It is critical that your workflows be able to survive and persist through these changes. This is where having extensive, up-to-date documentation of how processes are done and *why* processes are done is vital to the longevity of your program. That documentation should include what *positions* are responsible for each step in the process. That way, if a person leaves your organization, you can better determine who should do the work in the interim and what skills should be included on the job description of the new person being hired.

Table 7.1
An example permissions document that includes the user, what they have permission to, and how far that permission extends

User	Username	Role	Dark Archive			Working Files			Use Copies		
			Read	Write	Delete	Read	Write	Delete	Read	Write	Delete
Suzy Q	suzy.q	student worker	no	no	no	no	no	no	yes	no	no
Kirk McCoy	kirk.mccoy	digital archivist	yes	yes	yes	yes	yes	yes	yes	yes	yes
Jane Doe	jane.doe	oral historian	yes	yes	no	yes	yes	yes	yes	yes	yes

When leadership changes, this documentation can be used to help advocate for the continuation of your current program or for an increase in resources to expand your digital preservation efforts. Change is inevitable. Strong workflows and documentation can help you weather changes much more easily and efficiently.

Resource Allocation

When considering resource allocation, I am encouraging you to consider how you budget your financial resources, staff time, knowledge, and technological resources devoted to the ongoing maintenance and access of your digital materials. With digital materials, it is easy to become hyper-focused on financial resources dedicated to ongoing storage costs, subscription costs for digital asset management systems or other software used to preserve and provide access to your digital content, and the costs of equipment. However, another vital resource that needs to be managed is personnel time and knowledge.

At many institutions, staff are being asked to learn new skills and perform new tasks while maintaining their existing workload. In other scenarios there is one expert who is expected to be responsible for almost every aspect of digital content management, with some help from information technology departments. Perhaps you have a situation that is both: a staff member has been asked to become the expert and take over the responsibilities of digital preservation on top of their current responsibilities. This sets an institution up for gaps in preservation management when the expert leaves or when staff have to reprioritize their workload and digital preservation is put at the bottom of the list. So, just as you budget money, you need to budget staff time and expertise.

Spread out the responsibilities and expertise among multiple staff members as much as possible so that the pieces of digital preservation each person is asked to do fit well with their existing knowledge base or job responsibilities. Dedicate resources to training and continuing education for staff because the standards and practices of digital preservation are constantly changing simply due to the nature of the rapid evolution of digital materials. Encourage team building and communication between the archival and curatorial experts and the information technology experts. They have to work together to preserve digital content. It is easy for information technology experts to become overburdened by requests for expertise and resources specific to digital preservation in addition to the information technology department's existing workloads, so be deliberate about how digital preservation is added to that. Remember, the more content you add to your collections, the more resources you will need to allocate to the digital preservation effort. If you cannot sustain your digital preservation program on your current level of resources—financial, technological, and personnel—prioritize preserving the materials that you currently have and do not accept new accessions.

Notes

1. Sarah Higgins, "The DCC Curation Lifecycle Model," *International Journal of Digital Curation* 3, no. 1 (2008): 134–40, https://doi.org/10.2218/ijdc.v3i1.48.
2. "Levels of Digital Preservation," National Digital Stewardship Alliance, Digital Library Federation, http://ndsa.org//publications/levels-of-digital-preservation/.
3. "Fixity Pro," AVP, https://www.weareavp.com/products/fixity-pro/.

Chapter 8

Conclusion

The intent of the previous chapters is to provide you with a road map of how to move from the extensive corpus of digital preservation theory and standards into a practical set of workflows for your institution. Remember, digital preservation is iterative. Building out these workflows is only the first step. Every time you use a workflow, you may unintentionally modify it to work better, so be careful to track any consistent deviations you take from the workflow and build those new pathways in. A workflow that does not adapt to your current circumstances is of no use at all. Remember to document everything: what is done at each step, who is taking the step, and what tools are used to complete the step. Be careful to include any handoffs as their own step. It may be obvious now that when the content includes oral histories, the digital archivist will contact the oral historian to begin the processing workflow after the materials have been stabilized. What happens if the digital archivist was recently hired and therefore does not know oral histories require different expertise during processing?

Creating and maintaining these digital preservation workflows will act to do more than document existing practice. The process of creation will bring your team together and help build and maintain crucial relationships and shared understanding. In creating this documentation, you will learn how various types of professionals use language. I can say from experience that a digital archivist and an information security specialist have very different definitions for the term *archive*. Having a common understanding of terms in documents that have to be shared across professions is crucial to the success of your efforts. These documents create a common understanding of programmatic needs and will help different departments simultaneously advocate to administrators for critical technology, staff, and monetary resources to maintain and improve your digital preservation ecosystem. The end result of all of this effort is being able to provide digital cultural heritage materials to users now and in the future, so the process is worth the outcome.

Notes

Library Technology
R E P O R T S

Upcoming Issues	
July 57:5	**Digital Repositories with Cloud Technology** by Jarrod Bogucki
August/ September 57:6	**Metadata Applications Profiles for Library Data** by Theo Gerontakos and Ben Riesenberg
October 57:7	**Gigabit Libraries and Beyond** by Carson Block

Subscribe
alatechsource.org/subscribe

Purchase single copies in the ALA Store
alastore.ala.org

alatechsource.org

ALA TechSource, a unit of the publishing department of the American Library Association