CURATING COMMUNITY
DIGITAL COLLECTIONS

Digital Storage 3-2-1 Plan

After your digital files are gathered and organized so you know where and what they are, it’s time to make multiple copies of your master files and store them in multiple locations. *Remember “LOCKSS: Lots of Copies Keep Stuff Safe!”*

The 3-2-1 Rule[1]

3: Make *3 copies*. One copy can be the files on your hard drive, but also make 2 additional copies of all the files you want to save.
2: At least 2 of the copies should be on *2 different types of storage media*. If one copy is on your computer’s hard drive, and another is on an external hard drive, the third could be in cloud storage.

1: Store 1 of the copies in a *different location* from the other 2 copies. In the case of a fire, flood or other disaster, you’ll want to have a back-up in a different geographic location. This could be an external hard drive that you keep with a peer organization in another county, for example.

And some more rules . . .

- Keep your master files (the high-quality, large files in stable formats like TIFF or WAV) *separate from* your access files (the smaller files, like JPEG or MP3, you use for quick access, sharing online, etc.).
- Do not access the master files unless absolutely necessary (think “cold storage”).
- Restrict who has access to your master files. Accidents happen!
- Audit and update your storage media regularly. For example, external hard drives have a shelf life of 3-5 years.

Copy	**Media Type**	**Location**	**Date stored**	**Audit schedule**	**Fixity check schedule**	**Hardware replacement schedule**
Copy One						
Copy Two						
Copy Three						

[1] Adapted from “Personal Digital Archiving Guide Part 1: Preservation Planning,” David Scott David Witmer, University of Michigan Libraries
https://www.lib.umich.edu/blogs/bits-and-pieces/personal-digital-archiving-guide-part-1-preservation-planning

Checklists for Annual Auditing of Storage Media

External hard drives or other removable media:

- ❑ Mount the drive to make sure it still works.
- ❑ Open a sample of files to make sure that your system can still render them. If not, replace the corrupted file with a version you know is still good from one of your two redundant copies.

Network Attached Storage/local server:

- ❑ Check on the backup protocols established for your server. If it is networked, someone is managing it and likely has a schedule of backups they follow. How often? To what media?

Cloud storage:

- ❑ Who in your organization has access? Where are user name/password/other authentication stored?
- ❑ What is the viability of this service provider over the next 1-3 years?
- ❑ Pull down samples of your files to make sure that your system can still render them. If not, replace the corrupted file with a version you know is still good from one of your two redundant copies.