Digital Preservation

It is a common misconception that once something has been digitized and put online, it will be there forever. In fact, digital records are just as fragile as analog records, if not more so! Preserving digital records for the long haul requires active, continual management.

This webpage will:

- Give you a quick introduction to some basic digital preservation concepts
- Tell you what we are doing to protect UPLINK records
- Explain the benefits of the Michigan Digital Preservation Network and LOCKSS systems
- Tell you what you can do to protect your own digital files

Introduction to Digital Preservation

Digital files are in danger from a large number of risks. These risks include:
- Failure of hard drives: Digital files are still made up of physical bits. Like any other equipment, hard drives age and fail over time.
- Human error: Accidental deletion of files, accidental editing of files, dropping hard drives, etc.
- Obsolescence of hardware: When companies stop making hardware (ex: floppy disk drives), it becomes increasingly difficult to access files kept on the medium that corresponds with that hardware (ex: floppy disks).
- Obsolescence of software: When a company discontinues software or goes out of business, it quickly becomes difficult to access files made using that software.
- Obsolescence of file formats: Some file formats are proprietary and owned by the companies that created them (ex: Word Perfect files). If the company that makes the format disappears or discontinues a software program that saves files in that file format, the file formats rapidly go obsolete as other software programs stop supporting that file format as well.
- Corruption of files: Errors or unintentional changes to a file that occur when it is accessed, transferred, or stored. 1 in 1500 files have some level of corruption after 6 months according to a [2007 CERN study](#)!
- Natural disasters: Fires, floods, and other natural disasters can destroy digital files as well as physical ones.

There are a number of digital preservation strategies to guard against these risks. Some of these strategies are:
- Using open-source and/or popular file formats: If a file format is open-source (not owned by a corporation), then it is likely to survive over time and be supported by many

software programs. Popular file formats are also likely to be well-supported over time because of the sheer volume of records made using them.

- Backups: Keeping multiple copies of digital files so that if one copy is corrupted, another copy still survives.
- Geographical Separation: Keeping a copy or copies of digital files in another physical location so that if the hard drives at one location are destroyed by a natural disaster, the files still survive in the other location.
- Fixity Checks: Running regular checks to see if a file has been corrupted.
- Refreshing: Transferring the files onto a new hard drive or other storage medium once the old one is approaching the end of its expected lifespan.
- Migration: Moving the content from one file format to another because of the obsolescence of the hardware or software needed to access it or the obsolescence of the file format itself.

Want to learn more about digital preservation? Here are some resources:
[Digital Preservation Coalition Handbook](#)
[Digital Preservation: An Introduction to the Basic Concepts webinar](#)

What We Are Doing to Protect UPLINK Records

- We will save all digital records as open-source/common file formats. You can learn more about what file formats we use on the [Digitization page](#).
- We will maintain one access copy of your files on our server as well as two preservation copies on two different hard drives.
- We will do regular fixity checks every six months to find corruption.
- We will refresh our hard drives every seven years.
- If one of the file formats that we use for digitization is going obsolete, we will migrate the files to a new file format.

These measures will protect against individual hardware and file failures. However, they will not protect your files against system-wide failures or natural disasters. To do that, we need geographically separated copies of the files. UPLINK plans to join the new MDPN (Michigan Digital Preservation Network), but its system is not yet in place. Another way to ensure geographical separation is to commit to doing digital preservation for copies of your own digital records. See the sections below for more information.

MDPN and Benefits of LOCKSS

UPLINK is planning to join the new Michigan Digital Preservation Network (MDPN). The MDPN uses a software called LOCKSS (Lots of Copies Keeps Stuff Safe) to send copies of your

records to several archives around the state of Michigan. These copies of your records will not be used but will be maintained as backups in case any of the other copies fails. The MDPN is still in development, but should be up and running in the next year.

Learn more about the Michigan Digital Preservation Network [here](#).

Learn more about LOCKSS [here](#).

What Can You Do to Protect Your Own Digital Records

Basic

Keep and continue to care for the original analog copy of your digitized records if at all possible.
It is always possible that all of the digital versions of your records will be lost. Maintaining the original records ensures that the content will not be lost (and ensures that we can re-digitize the records if you wish).

Maintain your own backup copy of your digitized records.
As mentioned above, geographic separation of copies of digitized records adds an extra layer of protection. If a natural or manmade disaster were to take out all of UPLINK's hard drives, the digital records would still survive on your hard drive. UPLINK can send you an extra backup copy of your digitized records. Even by just holding onto this backup copy and doing nothing else, you are making it more likely that your digital records will survive long-term.

Advanced

If you want to do more to preserve your digital records, an UPLINK staff member can teach you how to create a digital preservation plan for your copies of your digitized records including:
- Deciding how many backups to keep and where to keep them
- Doing regular fixity checks on your backup copies to make sure that they aren't corrupted
- Refreshing your backup media periodically