DIGITAL PRESERVATION GUIDELINES

O·W·L·S
Local Libraries • Better Together

PHOTO BY V. H. RHODES, HORTONVILLE,

CORRESPONDENCE HERE

Hello Everybody:- Will
come Thurs. morning
in meanwhile be good
all of you, Harry too. Don't
he feel a little lonely for
me, I do, I have got such
a cold and feel so grippy
but will be all right if I
only reach the [illegible] again

NAME AND ADDRESS HERE

FEB 11 ELAND

FEB 11 1905 E.

Mr Frank Schu
Eland
Wis
R.R. I Box 21.

Digital Preservation Guidelines

What is Digital Preservation?

“Digital preservation combines policies, strategies and actions to ensure the most accurate rendering possible of authenticated content over time, regardless of the challenges of file corruption, media failure and technological change. Digital preservation applies to content that is born digital or converted to digital form.”[1]

[1] http://www.ala.org/alcts/resources/preserv/2009def

Long-term Digital Preservation

What is long-term preservation?

A period of time long enough for there to be concern about the loss of integrity of digital information held in a repository, including deterioration of storage media, changing technologies, support for old and new media and data formats, and a changing user community. This period extends into the indefinite future

When considering how to preserve digital data, you should address these questions:

- Where are the data stored?
- Do you store a copy of the data off-site?
- How do you ensure the integrity of the data over time?
- What IT security features are required for storing and accessing the data?
- What additional IT security features do you need?
- What metadata standards should be used to document the data?
- What sustainable file formats should be used for long-term storage?
- Who can you ask for assistance?

What is sustainable format?

The ability to access an electronic record throughout its lifecycle, regardless of the technology used when it was originally created. A sustainable format is one that increases the likelihood of a record being accessible in the future.

Format will change over time, some file formats will become obsolete. Before these formats become obsolete, it is important to migrate the materials to a format that will be readable in the future. Since formats are constantly changing, this preferred formats listed below will need auditing every two years to ensure that file formats do not become obsolete.

Suggested File Formats

- .TIFF or .JP2 (JPEG 2000) for archival preservation
- .JPG for access copies
- .XLS for metadata
- .TXT for OCR

Levels of Digital Preservation

https://ndsa.org//activities/levels-of-digital-preservation/

	Level 1 (Protect your data)	Level 2 (Know your data)	Level 3 (Monitor your data)	Level 4 (Repair your data)
Storage and Geographic Location	- Two complete copies that are not collocated - For data on heterogeneous media (optical discs, hard drives, etc.) get the content off the medium and into your storage system	- At least three complete copies - At least one copy in a different geographic location - Document your storage system(s) and storage media and what you need to use them	- At least one copy in a geographic location with a different disaster threat - Obsolescence monitoring process for your storage system(s) and media	-At least three copies in geographic locations with different disaster threats - Have a comprehensive plan in place that will keep files and metadata on currently accessible media or systems
File Fixity and Data Integrity	-Check file fixity on ingest if it has been provided with the content -Create fixity info if it wasn't provided with the content	- Check fixity on all ingests - Use write-blockers when working with original media - Virus-check high risk content	- Check fixity of content at fixed intervals - Maintain logs of fixity info; supply audit on demand - Ability to detect corrupt data - Virus-check all content	- Check fixity of all content in response to specific events or activities - Ability to replace/repair corrupted data - Ensure no one person has write access to all copies
Information Security	- Identify who has read, write, move and delete authorization to individual files - Restrict who has those authorizations to individual files	- Document access restrictions for content	-Maintain logs of who performed what actions on files, including deletions and preservation actions	- Perform audit of logs
Metadata	- Inventory of content and its storage location - Ensure backup and non-collocation of inventory	- Store administrative metadata - Store transformative metadata and log events	-Store standard technical and descriptive metadata	-Store standard preservation metadata
File Formats	- When you can give input into the creation of digital files encourage use of a limited set of known open formats and codecs	- Inventory of file formats in use	-Monitor file format obsolescence issues	- Perform format migrations, emulation and similar activities as needed

Scope and Rationale

The purpose of this policy is to create a framework reflecting a set of policies that show OWLS commitment to the stewardship and preservation of digital assets. These digital assets are an important part of our cultural heritage. Their existence is at risk unless formal commitment to their preservation is articulated, developed, and implemented. This formal commitment protects the investments we have all made over the years in acquiring and creating digital collections.

OWLS is looking to reach a level one in the National Digital Stewardship Alliance's Levels of Digital Preservation. OWLS is looking to collect an archival copy of digital objects, as well as any accompanying metadata and OCR files. OWLS is not looking to collect the only copy of the digital object. Each site is still responsible for the care of their digital assets. These policies and accompanying workflow will help address how to care for your digital assets.

Care of Physical Materials

Digitization does not equal preservation. Just because you are working to digitize a collection, does not mean that the materials themselves do not need to be physically preserved. OWLS recommends that materials be kept in archival safe folders and archival boxes. Gaylord Archival has great options to store your physical collections. If you have any questions on preservation, contact OWLS.

Roles and Responsibilities

The OWLSnet Manager will be the main entity responsible for the care of the digital objects for preservation. The OWLSnet Manager's responsibilities include:

- Running Exactly and Fixity
- Moving digital objects to appropriate storage for digital preservation
- Updating the inventory spreadsheet
- Monitoring the checksums
- Migrating items to new storage when the hard drives are reaching obsolescence

Audits and Review

Digital Preservation Guidelines and Digital Preservation Workflow

The Digital Preservation Guidelines and Digital Preservation Workflow are subjected to audit every two years. This ensure that best practices are being met and stay aligned with the changing landscape in digital preservation.

Expected date of review: August 2020

Digital Storage Audits

Every 3 years, the OWLSnet Manager is responsible for migrating digital objects from the current hard drives to new external hard drives. External hard drives have a short life span. At this time, the OWLSnet Manager will review storage options and make recommendations.

Expected date of audit: August 2021

Checksum Audits

Every year, the OWLSnet Manager is responsible for checking the checksums to make sure that all digital objects are not becoming corrupt and still have the original integrity as the day there were scanned.

Expected date of audit: August 2019

Storage Options

Storage Options for OWLS

OWLS is the main source for preserving digital object of cultural significance. OWLS will be following two main principles of digital preservation: LOCKSS (Lots of Copies Keep Stuff Safe) and the 3-2-1 Rule. To achieve this, OWLS will be keeping an archival copy of the member libraries digital collection and storing them in three ways:

1. External Hard Drive (not connected to the server)
2. Server at OWLS
3. Cloud Storage (Box)

Recommended Storage Options for Libraries

OWLS recommends that each library have two external hard drives for storage of their digital collections. The external hard drives need to be updated every 3 years to ensure they do not become obsolete and corrupt. As an advanced safety precaution, find external hard drives that are made by two different companies.

Concerns to be addressed:

Digital storage is a constantly changing. OWLS recommends that you look at your current external hard drives to address any concerns in regards to the age. External hard drives have a short life span of about 3-5 years. Err on the side of caution, replace your hard drives if they are 3 years old.

Thumb drives are not appropriate storage. They have a shorter lifespan than external hard drives. They are prone to corruption, transferring viruses, and corrupting digital files. Address this concern as soon as possible.

Optical media (DVDs, CDs, Archival Gold Discs) are not appropriate storage. They have an extremely short life span, as well as many new computers not supporting optical discs as they do not have disc drives. Address this concern as soon as possible.

Transfer of Digital Objects to OWLS

Transferring digital collections to the OWLSnet Manager can be done two ways:

1. Transferring via external hard drive
2. Transferring via WeTransfer

When transferring files, let the OWLSnet Manager know which way you will be transferring files. OWLS will not be transferring files via thumb drives. To request an external hard drive be sent to you for file sharing, please contact Amanda (alee@owlsweb.org). When sending new digital collections, please fill out a collection inventory and send this with your digital collection.

Who to Contact

For any questions, or concerns, contact the OWLSnet Manager, Amanda, at alee@owlsweb.org