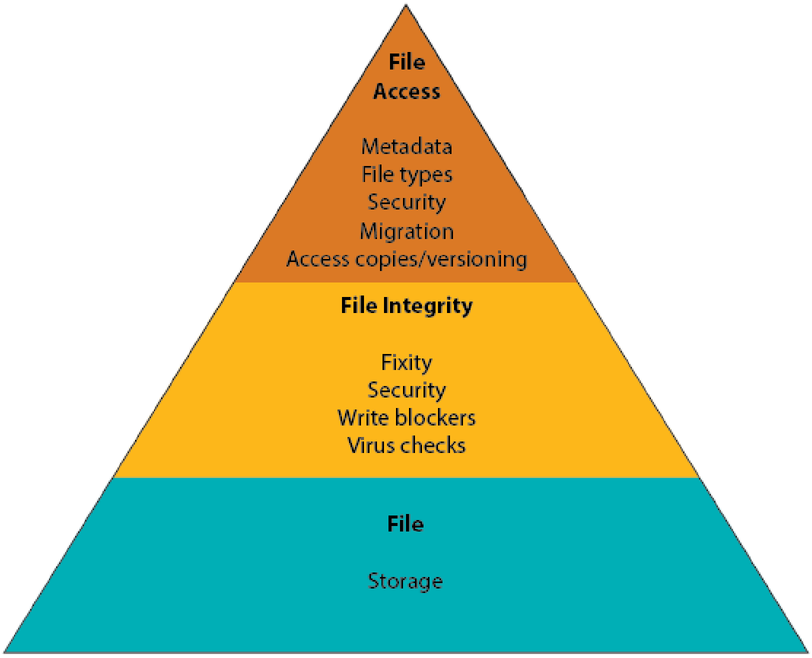
[Insert Institution and Department Name]
Digital Preservation Plan
[Insert Date]
Digital Stewardship Curriculum

Digital Preservation is the long term storage and care of digital files, making sure that digital information remains accessible and usable over time. Digital Preservation combines strategies and actions to ensure access to digital files in the best way for each institution, despite challenges of technological changes and media failure. Digital files might come into your institution in a few ways:

- Digitization - Creating digital surrogates of original physical materials, in your institution or elsewhere.
- Donation - Accepting donations of digital files (which may be digital surrogates or be born digital).
- Creation - Your institution may create digital files by conducting oral histories, writing transcripts in a text document, or taking digital photographs of an event.

For any institution or department, it is essential that a **Digital Preservation Plan** is created and followed for any digital content that should be preserved in the long term. Having a plan, and regularly updating it, will increase the sustainability, accountability, and flexibility of digital projects.



The Digital Stewardship Curriculum divides Digital Preservation into the sections of **File Storage**, **File Integrity**, and **File Access**. Making a preliminary plan that covers these sections and subsections will be a start to developing a formal Digital Preservation Policy, or adding Digital Preservation concepts into other policies.

Fill out each section to the best of your ability. If you are unsure of a subsection, review digital preservation slides, handouts, and activities within the Digital Stewardship Curriculum.

Plans for review/updates of Digital Preservation Plan:

Digital Preservation: File Storage

- Responsible departments and positions:

Who is responsible for storage and backup of digital files?

*Remember the 3-2-1 rule (3 copies of any information you want to preserve long term, stored on 2 different types of media, 1 in a different geographic location)

- Primary Storage:

- Secondary Storage:

- Tertiary Storage:

- Backup schedule:

  When will files be backed up to the three storage steps (weekly, biweekly, monthly, etc.)? Who will do the work of transferring?

- Funding for storage:

  Where does funding come from for purchasing storage media? Do you need to seek funding before purchasing any media?

- Technical support for storage:

  Who is responsible for setup and maintenance of storage media?

- Versions of your files (preservation masters, access copies, derivatives):

  Specify what versions of files will exist, and then which of those versions will be backed up in your preservation plan. For example: "Only preservation masters are preserved."

- Disaster planning:

  Outline what will happen if disaster strikes. List possibilities: what are all the types of natural disaster, human error, or media failure that could occur. Then your plan for dealing with a disaster. Who will be responsible for damage assessment and recovery? How will files be recovered? This type of information should be thought out, then included in your overall disaster plan for your institution.

Digital Preservation: File Integrity

- Responsible departments and positions:

  Who is responsible for integrity of digital files?

- Fixity:

  How will you run fixity checks - what tool or tools will you use? Where will fixity information be stored? At what points in your workflow will you create and verify fixity information?

- Security:

  Who is responsible for security of digital files? Who has access to move, delete, or change digital files? How are security measures enforced through policies, procedures, and actions? This might include everything from if passwords are used on office computers to if digital storage media is kept locked in a secure area.

- Write blockers:

  Using a writeblocker helps show authenticity, and that no files were changed when copying from from storage one media to another. Do you have a plan to use a hardware or software writeblocker when accepting new digital files from donors?

- Virus Checks:

  Are regular virus checks run on all office computers? Who is responsible for fixing if a virus is found? When processing donated digital materials, is there a non-networked computer that can be used for file transfer? (Many digital storage formats, such as flash drives, are vulnerable to viruses and must be processed carefully).

- Funding for file integrity (if needed):

  What is the source of funding for any software or hardware needed for file integrity steps?

- Technical support for file integrity:

  Who is responsible for setting up, managing, and implementing file integrity hardware, tools, or processes?

- Disaster planning:

  Plan out what will happen related to file integrity after a disaster event. Specifically, have a plan for running fixity checks, comparing files based on checksums, and creating new checksums if needed.

Digital Preservation: File Access

- Responsible departments and positions:

  Who is responsible for access concerns of digital files?

- Metadata:

  What preservation metadata is collected for digital files? What standards are followed? Where/how is the metadata stored? Who is responsible for creating and checking metadata? Do you have multiple levels of metadata (for example: basic inventory, descriptive, technical, preservation, administrative)?

- File types:

  What file types have you decided on for the different formats and versions of digital files in your collections? How will you instruct your donors about file types for digital donations? Will you convert files to your standardized formats if needed?

- Migration:

  Consider two types of migration: storage and file type. How will you know when it is time to get new storage media and migrate content? How will you keep updated on file types and when you might need to perform a mass conversion of files to keep up with technology?

- Funding for file access (if needed):

  What is the source of funding for any software or other tools needed for file integrity steps?

- Technical support for file access:

  Who is responsible for setting up and managing file access tools or processes?