



# Storage

**Back-up:** A copy of your digital content, ideally stored in a different location from the original, usually made to prevent data loss.

**Preservation:** The “series of managed activities necessary to ensure continued access to digital materials for as long as necessary”. –*Digital Preservation Coalition*

Where and how you choose to store your research materials and writings will determine how long they survive. To mitigate against loss, make your own back-ups on a regular, formalized schedule (e.g. daily or weekly).

### Threats to storage environments:

- Natural disaster
- Human error
- Human malice
- Drive failure
- Format obsolescence
- Media obsolescence
- Bit rot
- Business failure
- Software or hardware error

### Basic recommendations:

1. Maintain at least one local (i.e., non-cloud-based) copy of your content
2. Maintain at least three separate complete copies of your research content
3. Maintain at least one copy in a different geographic location
4. Maintain a history of changes in at least one location (e.g., using a “Time Capsule” software package to automatically back up your content without deleting older copies)
5. Document in a text file how, when, and where you store and back up your materials
6. Systematize your folder- and file-name conventions using human-identifiable information
7. Use naming conventions to mark versions of files, e.g., using consecutive numbers to track a file through all edits and revisions that take place to it. (e.g., filename-v12.txt)
8. Make sure your filenames are followed by the correct file extension (e.g., .txt, .csv)
9. Avoid using special characters in all file and folder names (e.g., \?:\*?<>{}[]&\$.;,:!)
10. Document the formats you are managing and the potential sustainability issues
11. Save a copy of your research files in non proprietary formats, so that you don’t need a software license to render and use them.

### Advanced recommendations:

1. Produce and maintain an inventory of all of your content, documenting file names, sizes, locations, and types
2. Create and regularly check “checksums” or digital signatures for your most important research files. Checksums can be generated by several open source tools and utilities and they can be stored in your inventory.
3. Monitor your content to ensure missing, moved, and renamed files are automatically brought to your attention. A tool like “[Fixity](#)” can scan specified folders or directories on a regular basis and report changes to you via email.

### Resources

1. For “back-up” advice, see Jesus Vigo, [Best Practices to Back up Your Data](#)
2. For more on cloud-based backups, please see Charles Beagrie Ltd. [How Cloud Storage can address the need of public archives in the UK](#)
3. For general information, see also [Personal Digital Archiving](#)

