

# Digital Preservation at Oxford and Cambridge

A collaborative research project to evaluate and provide sustainable recommendations for our digital preservation programmes

## Digital preservation with limited resources

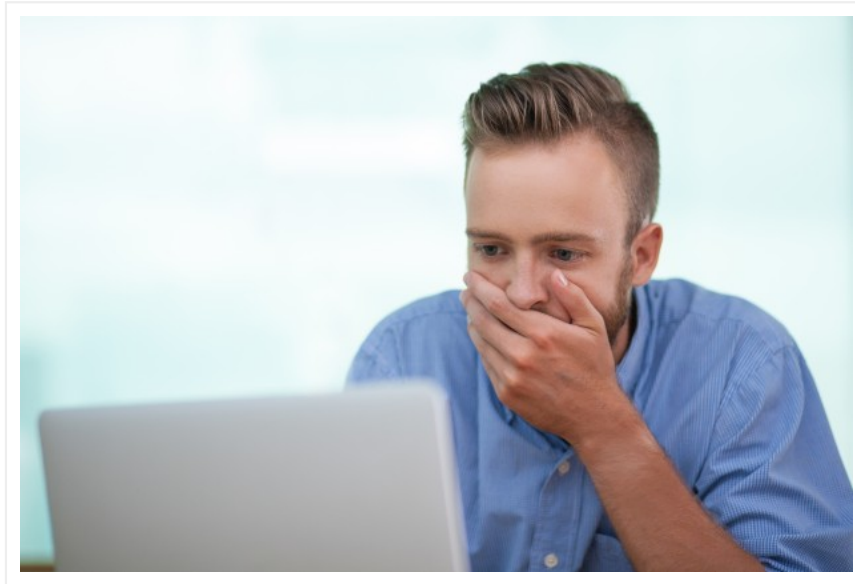
Posted on [18 May, 2018](#) by [ehalvarsson](#)

***What should my digital preservation strategy be, if I do not have access to repository software or a DAMS system?***

At Oxford, we recently received this question from a group of information professionals working for smaller archives. This will be a familiar scenario for many – purchasing and running repository software will require a regular dedicated budget, which many archives in the UK do not currently have available to them.

So what intermediate solutions could an archive put in place to better its chances of not losing digital collection content until such a time? This blog summarises some key points from meeting with the archivists, and we hope that these may be useful for other organisations who are asking the same question.

***Protect yourself against human error***



— CC-BY KateMangoStar, Freepik

Human error is one of the major risks to digital content. It is not uncommon that users will inadvertently drag files/folders or delete content by mistake. It is therefore important to have strict user restrictions in place which limits who can delete, move, and edit digital collections. For this purpose you need to ensure that you have defined an “archives directory” which is separate from any “working directories” where users can still edit and actively work with content.

If you have IT support available to you, then speak to them about setting up new user restrictions.

### ***Monitor fixity***



— CC-BY Dooder, Freepik

However, even with strong user restrictions in place, human error can occur. In addition to enforcing stronger user restrictions in the “archives directory”, tools like [Fixity from AVP](#) can be used to spot if content has been moved between folders, deleted, or edited. By running regular Fixity reports an archivist can spot any suspicious looking changes.

We are aware that time constraints are a major factor which inhibits staff from adding additional tasks to their workload, but luckily Fixity can be set to run automatically on a weekly basis, providing users with an email report at the end of the week.

***Understand how your organisation does back-ups***



— CC-BY Shayne\_ch13, Freepik

A common IT retention period for back-ups of desktop computers is 14 days. The two week period enables disaster recovery of working environments, to ensure that business can continue as usual. However, a 14 day back-up is not the same as preservation storage and it is not a suitable solution for archival collections.

In this scenario, where content is stored on a file system with no versioning, the archivist only has 14 days to spot any issues and retrieve an older back-up before it is too late. So please don't go on holiday or get ill for long! Even with tools like Fixity, fourteen days is an unrealistic turn-around time (if the issue is at all spotted in the first place).

If possible, try and make the case to your organisation that you require more varied types of back-ups for the “archival directory”. These should include back-ups which are *at least* retained for a

year. Using a mix of tape storage and/or cloud service providers can be a less expensive way of storing additional back-ups which do not require ongoing access. It is an investment which is worth making.

As a note of warning though – you are still only dealing in back-ups. This is not archival storage. If there are issues with multiple back-ups (due to for example transfer or hardware errors) you can still lose content. The longer term goal, once better back-ups are in place, should be to monitor the fixity of multiple copies of content from the “archival directory”. (For more information about the difference between back-ups used for regular IT purposes and storage for digital preservation see the [DPC Handbook](#))

### ***Check that your back-ups work***

Once you have got additional copies of your collection content, [remember to check that you can retrieve them again from storage](#).

Many organisations have been in the positions where they think they have backed up their content – only to find out that their back-ups have not been created properly when they need them. By testing retrieval you can protect your collections against this particular risk.

### ***But... what do I do if my organisation does not do back-ups at all?***

Although the 14 day back-up retention is common in many businesses, it is far from the reality which certain types of archives operate within. A small community organisation may for example do all its business on a laptop or workstation which is shared by all staff (including the archive).

This is a dangerous position to be in, as hardware failure can cause immediate and total loss. There is not a magic bullet for solving this issue, but some of the advice which Sarah (Training and Outreach Fellow at Bodleian Libraries) has provided in her *Personal Digital Archiving Course* could apply.

Considerations from Sarah’s course include:

- Create back-ups on additional removable hard drive(s) and store them in a different geographical location from the main laptop/workstation

- Make use of free cloud storage limits (do check the licenses though to see what you are agreeing to – it's not where you would want to put your HR records!)
- Again – remember to check your back-ups!
- For digitized [images](#) and [video](#), consider using the Internet Archive's Gallery as an additional copy (note that this is open to the public, and requires assigning a CC-BY license) ([If you like the work that the Internet Archive does – you can donate to them here](#) )
- Apply [batch-renaming tools](#) to file names to ensure that they contain understandable metadata in case they are separated from their original folders

(Email us if you would like to get a copy of Sarah's lecture slides with more information)

### ***Document all of the above***



— CC-BY jcomp, Freepik

Make sure to write down all the decisions you have made regarding back-ups, monitoring, and other activities. This allows for succession planning and ensures that you have a paper trail in place.

### ***Stronger in numbers***



— CC-BY, Kjpargeter, Freepik

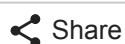
Licenses, contracts and ongoing management is expensive. Another venue to consider is looking to peer organisations to lower some of these costs. This could include entering into joint contracts with tape storage providers, or [consortium models for using repository software](#). An example of an initiative which has done this is the [NEA \(Network Electronic Archive\) group](#) which has been an established repository for over ten years supporting 28 small Danish archives.

### Summary:

*These are some of the considerations which may lower the risk of losing digital collections. Do you have any other ideas (or practical experience) of managing and preserving digital collections with limited resources, and without using a repository or DAMS system?*

---

### SHARE THIS:



This entry was posted in [baseline](#), [digital lifecycle](#), [digital preservation](#) by [ehalvarsson](#). Bookmark the [permalink](#)

[\[http://www.dpoc.ac.uk/2018/05/18/digital-preservation-with-limited-resources/\]](http://www.dpoc.ac.uk/2018/05/18/digital-preservation-with-limited-resources/) .

This site uses Akismet to reduce spam. [Learn how your comment data is processed.](#)