Nottingham Trent University (NTU) Research Data Storage: a guide

1. Introduction

Your research data are valuable assets; it is essential that you keep them safe and secure whilst you are still working on them. This guide will explain the facilities that are available to you at NTU and help you to identify the most appropriate storage for your digital data.

2. Best practice

Storing your research data according to best practice will not only offer sufficient data protection, but also enable you to work more flexibly, easily and quickly. The key to securing your data and maximising your efficiency during your research project is careful data management planning. Your data management plan [DMP] should outline where you plan to store your data and your data back-up strategy. Your storage arrangements must also be aligned with institutional and funder policies, and meet any relevant legal and ethical requirements.

2.1 Policies to help you

It is essential that you familiarise yourself with, and adhere to, the following University policies before forming your data storage strategy:

- Information Classification Policy
- *Data Security: Policy for portable devices and storage media*
- *Data Protection Policy*
- *Computer Use Regulations*

2.2 Data management planning

The type of storage that is most suitable for your research data is dependent on different factors; therefore, your storage requirements and solutions might vary from one research project to the next. When determining your approach to data storage, you should address the following in your DMP:

1. *The storage option/s you are going to use*
   Section 4 details the University-endorsed storage solutions that are available to you. Is there any risk that the data may be lost? How might you mitigate that risk?
2. *Volume of data*
   How much storage will you need and will this vary during the project? Does all of it need to be immediately accessible?
3. *Data classification*
   Are you working with personal, sensitive or confidential data? Personal data is anything that relates to an identified or identifiable individual. Sensitive data includes special category data as defined by the ICO, and data that is either commercially sensitive, or is likely to have a significant negative public impact if released. The University Information Classification Policy stipulates what storage is acceptable for different categories of data: highly confidential; confidential; open and public. For example, it states that you should not store any highly confidential or confidential data in OneDrive for Business or SharePoint.
4. *Data protection*
   Explain in your DMP how you will ensure the accuracy and consistency of the data, protect the system that holds the data and restrict access to the data. This

Version 1.1
January 2019
Jane Bonnell / Ian Slater

must be proportionate to the type of research data you are storing. For example, additional safeguards for personal or sensitive data, such as encryption, might be necessary.

5. *Accessibility of data*
   How and where will the data storage need to be accessed from? Are there any ethical/ legal/ contractual constraints on data access?
6. *Funding for data storage*
   Have you secured funding for data storage? Wherever possible you should include costing for research data storage in any funding proposals since there are costs associated with data storage that you should try to recover. To calculate your expenditure on research data storage for the duration of your project, please refer to *Funding support for research data storage costs.*
7. *Collaboration: internal or external*
   Who needs to access your data? Are they researchers from within, or external to, the University?

You will also need to plan for the long-term storage of any valuable data that either underpins any research outputs or has potential for future reuse. NTU's Research Data Management Officer will help you to explore your options for preserving and sharing your research data.

2.3 Backing up your data

Your DMP should document your data back-up protocols, including how regularly back-ups will take place. Minimise the risk of data loss and corruption to your data resulting from hardware failures, theft and viruses by applying the 3-2-1 Rule: keep three copies of your files in two different locations, with one copy off-site, ideally in a different geographic location.

3. Overview of active research data storage options

Storage option	Automatic backup?	Shared within NTU?	Shared outside of NTU?	Suitable for sensitive data?	Scalable?
OneDrive for Business	NO	YES	YES	NO	NO
NTU DataStore	YES	YES	YES	YES	YES
SharePoint	NO	YES	YES	NO	NO
Local drives on PC/ Laptop	NO	NO	NO	YES- Temporarily & only if encrypted	NO
External Portable Storage Devices	NO	NO	NO	YES- Temporarily & only if encrypted	NO
Personal cloud storage	NO	YES	YES	NO	NO

4. Active Research Data Storage options provided by NTU

4.1 OneDrive for Business

At NTU, you are automatically provided with 5TB of storage through OneDrive for Business. This offers:

- access to your data anytime, anywhere using multiple devices;
- automatic file syncing across all of your devices;
- sharing and collaborative functionality, so you can share files and set permissions for multiple people to edit documents;
- GDPR compliant data privacy and security measures;
- file recovery from your recycle bin for up to 90 days, so you can retrieve deleted files;
- the retention of at least one hundred major versions of each document, therefore it is possible to restore previous versions of each file;
- an account that is managed by NTU through a service agreement with Microsoft and accessed through your University log-in details. This type of account is different from personal cloud based services, such as OneDrive, Dropbox and Google Drive, which are not endorsed for research data storage for the reasons outlined in Section 5.4.

Things that you should consider:

- Data is not backed up, therefore you should store another copy of the data in another location.
- OneDrive for Business is available only for your period of employment at the University; therefore, the account and/or shared files become unavailable if you, or a researcher you are collaborating with, leave NTU.
- It is possible to sync files to private devices to which you won't always have control; therefore, personal, sensitive or confidential data should not be saved within OneDrive for Business.
- If you have funding for active research data costs then you should store your data in the NTU DataStore (see Section 4.3). Similarly, if you are preparing a funding bid you should plan to store your data in the NTU DataStore and, where the funding body permits, include the costs for using this storage in your proposal.

In summary, despite the advantages offered by OneDrive for Business, this cloud-based service may not be appropriate if your research has additional security or technical requirements. Therefore, you should request alternative data storage arrangements (see Sections 4.2 and 4.3) if your research meets one, or more, of the following criteria:

- There is any personal, sensitive or confidential data;
- It is a collaborative research project;
- The amount of data generated is expected to exceed 5TB.

Section 6 explains the process for requesting different storage solutions.

4.2 SharePoint

SharePoint might be the best option for data storage if your research necessitates:

- *Collaborative functionality*
  SharePoint facilitates the sharing of documents with colleagues, both internally and externally. You can share entire sites, folders, and/or individual files. As a site administrator, you can easily assign different permissions to different users. For example, you can give some collaborators read-only or full editing privileges.
- *Accessibility*
  SharePoint is an excellent storage option if you require the use of a range of

different devices. It is compatible with tablets, smartphones, netbooks and desktops, offering ease of access to your account from any internet connection.

Things that you should consider:

- SharePoint, like OneDrive for Business, is not suitable for personal, sensitive or confidential data.
- Data is recoverable from your recycle bin for up to 90 days and SharePoint retains at least 100 major versions of each file to allow for the restoration of previous versions. However, data is not backed up, therefore you should store another copy of the data in another location.
- If you have funding for active research data storage, then a more robust and secure solution is the NTU DataStore (see Section 4.3).

4.3 NTU DataStore

This is the University's centrally managed storage service. It provides the most secure environment for your data by offering:

- *Automatic back-up*
  It follows the 3-2-1 rule as the data is replicated between the 3 different university campus sites. Therefore, you do not have to implement additional back-up protocols.
- *Local data storage*
  Data is stored on NTU servers, as opposed to being cloud based which is why it is the only option for personal, sensitive and confidential data.
- *Resilience*
  It is managed and kept secure by IS, so you do not have the responsibility of routinely testing the storage system.
- *Accessibility*
  You can access this service both on campus and remotely via a virtual private network (VPN).
- *Collaboration*
  You are able to share your folders with internal and external collaborators. You can request that users have different permissions within the storage, therefore you can restrict access to certain folders and assign different editing privileges where necessary.

Things to consider:

- It costs 10p per GB/ £100 per TB per year to store data in the NTU DataStore. It is important that you plan for this from the very outset of each project. Your DMP and funding proposal should include costs for data storage in order to try to recover these expenses. For further information, please consult *Funding support for research data storage costs,* or contact NTU's Research Data Management Officer.
- Even if you do not have funds to recover storage costs, you must request space on the NTU DataStore if your research involves personal, sensitive or confidential data.
- You will need to arrange for a Sponsored Account to be created for each of your external collaborators. To do this, please contact the IS Service Desk.

5. Other options

The storage solutions in this section are not recommended. If used at all, they should only be used as temporary storage, or as part of your back up procedure when using OneDrive for Business and/or SharePoint. Please seek advice from NTU's Research Data Management Officer if you are planning to use any of these methods for your data storage.

5.1 Local drives

Storing data on the hard drives of workstations, PCs and laptops is a good solution if you are working in the field, are working on your data, or you need to save a copy of key data. However:

- The device must use whole disk encryption;
- Mobile devices are particularly vulnerable to loss, theft, or breakage so you will need to back up your data using another method;
- This solution doesn't facilitate collaboration.

5.2 Network Attached Storage (NAS)

NAS must not be connected to the NTU network, but can be locally attached to a PC. They are expensive, yet good solutions for large volumes of data and data collection fieldwork. You will need to address the following in your DMP:

- The device should have the event log and the file/full disk encryption enabled. The firmware and security needs to be regularly updated and any legacy/ insecure protocols should be disabled.
- You will need to back up the device; NAS are more resilient than single external drives, but there is a chance of data loss in the event of multiple drive failures and corruption.
- The portability of a NAS also presents a high risk to data security: the physical box can be lost or stolen.
- This solution does not facilitate collaboration.

5.3 External portable storage devices

External hard drives, CDs, DVDs and USBs are convenient, cheap and portable. However, they are not recommended for long-term storage as their longevity is uncertain and they can be easily damaged, lost or stolen. They need to be stored under the appropriate environmental conditions to minimise deterioration. They also do not facilitate collaboration. If you opt to use these, you will need to ensure that it is:

- physically secured and encrypted;
- regularly backed up.

5.4 Personal cloud services (OneDrive, Google Drive, Dropbox, iCloud Drive)

You should only use the University approved cloud storage service, i.e OneDrive for Business, for storing your research data. Personal accounts with cloud services are problematic for the following reasons:

- There is no guarantee of data confidentiality
- The data may be stored outside the European Economic Area, so will not be covered by EU data protection laws. In other jurisdictions, it may be accessed or removed without your knowledge or consent.
- There are no safeguards about the continuing existence of the data and no guarantee that your right to access it will be maintained.
- The data may be altered or corrupted without your knowledge, and you won't have any way of getting uncorrupted data back
- If the files are accidentally deleted there is no backup, nor are there any guarantees that the data is recoverable.
- Most cloud storage providers do not keep records of who has accessed or downloaded your data.

6. Requesting alternative data storage

For further information, or to discuss your active research data storage requirements in more detail, please contact NTU's Research Data Management Officer.

To apply for alternative storage arrangements for your research data, please complete the Active Research Data Storage Request Form and return it to the Research Data Management Officer at LIBReseachTeam@ntu.ac.uk.