School of Computer Science
Research Ethics Committee (CS REC)

Data Management Plan (DMP) Guidance

A data management plan must be put place for all research conducted at the University of Nottingham. If your research is part of a large project, a data management plan (including asset storage) may already have been created, please check with the project lead before completing the DMP form.

There are 2 key parts to implementing a data management plan:

1. Creating an **asset inventory** (a written document); see the Data Management Plan (DMP) form.
2. Creating **asset storage** (digital and / or physical); see below for guidance.

Staff may use University repositories,[1] or create their own asset storage on their University O365 account. Note that data stored in OneDrive will be deleted after the owner leaves the University; use a Team or SharePoint site with multiple owners if necessary.

UG, PGT and PGR students should always create digital asset storage on their University O365 account.[2]

Data assets may be stored on external drives as long as they are encrypted and backed up and reasonable steps are taken to ensure their physical security.

The DMP should be submitted to CS REC for audit purposes if ethics approval is required for the research (submit the DMP along with your ethics application).

[1] e.g., https://www.nottingham.ac.uk/library/research/research-data-management/index.aspx
[2] https://www.nottingham.ac.uk/dts/accounts-and-access/data-and-storage/data-and-file-storage.aspx

ASSET STORAGE (digital)

Please structure asset storage as follows.

Parent folder
Create a parent folder to contain your research data, give it a name (e.g., the project or study name) and record this name in the asset inventory. If your research is part of a larger project, the parent folder might be placed in a top-level asset folder for the whole project. If so, make sure you record this location in the asset inventory document too. Create the following folder structure within the parent folder. **Use the same numbers and names as set out below.**

1. Governance (University)
Put the asset inventory (DMP) in this folder and any documentation relevant to the governance of the data, e.g., confidentiality agreements, documents demonstrating that third party recipients or services comply with data protection regulation, data protection impact assessments, ethics documents (including versions and emails regarding revisions and approval), self-assessment and audit reports and emails, permissions to publish data, etc.

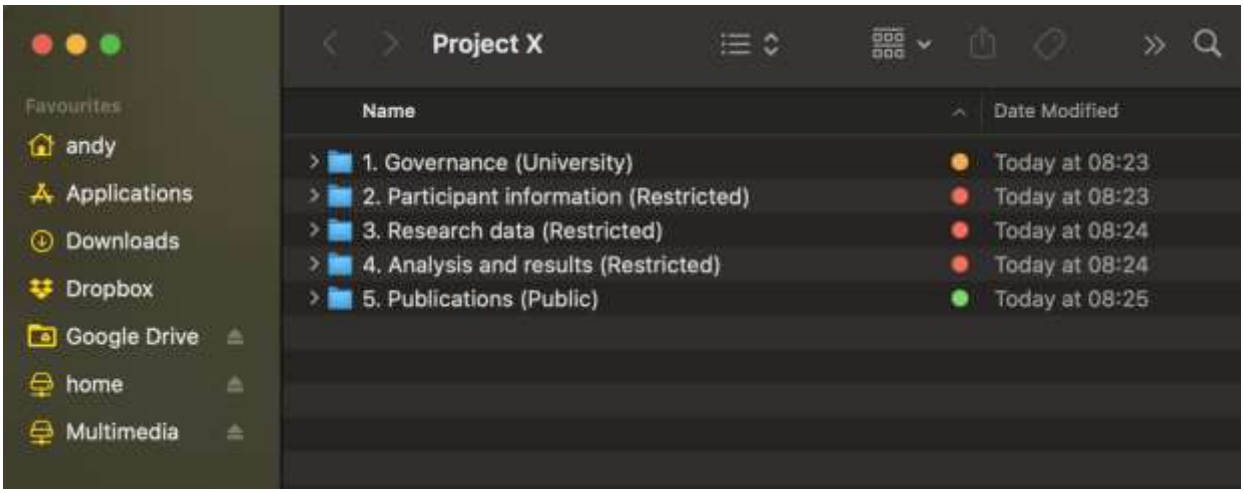
2. Participant information (Restricted)
Add copies/scans/photos of completed consent forms here, along with participant lists, records of withdrawals and any steps taken (e.g., data deleted). Include a log of consent permissions if the following applies that clearly indicates a) if joint copyright has been affirmed and b) if visual images of a participant should **not** be used in scientific works (presentations, reports or publications).

3. Research data (Restricted)
Add the data collected during the research here (e.g., audio/video recordings, logs with location or physiological data, survey response data, etc.). There may be several sub-folders here (e.g., for different types of data or different data collection sessions or experiments). You should clearly flag any visual data that identifies participants who have **not** consented to their visual image being used in scientific works (presentations, reports or publications).

4. Analysis and results (Restricted)
Add your analyses of the data here, including the outputs of data processing (such as transcriptions, statistics, marked up video extracts, etc.), working papers or reports. Again, there may be several sub-folders here (e.g., for different analyses or reports). Clearly flag if any processed data contains visual data that identifies participants who have **not** consented to their visual image being used in scientific works (presentations, reports or publications).

5. Publications (Public)
Add any publications that make use of the data here. Each publication should be hosted in its own folder along with the data used in the publication. If the data identifies or could identify participants (e.g., video or audio), a de-identified (anonymised or pseudonymised) version of the data (such as a transcript) should accompany the publication. Data placed here may be made available to others, including being posted online and hosted in data repositories. **It is CS REC policy that data which identifies or could identify people is not made available to others unless it was collected for such purposes and this was clearly specified and agreed to in the ethics consent form.** This policy may be cited in a publication's Data Access Statement. In short, you must not share data that identifies or could identify people with others outside the research team unless you have obtained consent.

By default, contents of the **participant information**, **research data**, and **analysis and results** folders should be restricted; contents of the **governance** folder may be shared with others in the University; contents of the **publications** folders have or could be made public.



ASSET STORAGE (physical)

Physical assets, including documents, memory cards, USB drives, CD-ROMS, etc., should be stored in physical locations as appropriate to the risks that attach to the data they contain. As identified in the asset inventory, special category data and identifiable or potentially identifiable data must be stored securely, not only in a locked office but a locked cupboard or filing cabinet. The location of such data must be specified in the asset inventory.[3]

Efforts should be made to minimise the number of printed documents containing special category data and identifiable or potentially identifiable data. It is considered best practice to **scan printed documents wherever possible** and store digital versions in the appropriate folder as described above and then destroy the original hard copies as explained below.

Security measures should be put in place to control access to physical assets. Keys should be held by data steward(s) named in the asset inventory. Access procedures should be put in place (e.g., a log of users accessing the physical asset should be kept). The security of the asset should be routinely checked (e.g., to make sure it is locked after use) to prevent inappropriate access.

Physical assets should only be taken off University premises with written permission from the data owner or data steward, and should not be reviewed in public areas. Anyone granted permission by the data owner or data steward to remove physical assets from University premises is responsible for their safe keeping and security, and their safe return to University premises.

Special category data and identifiable or potentially identifiable data must be destroyed in a secure way, either through shredding (cross-cut shredder) in the case of printed data or through the University's (free) secure disposal service. While awaiting destruction, physical data assets must be stored in a secure environment until collection.

[3] Special category data includes health, genetic and biometric data, and data about a participant's sexual orientation or sex life, racial or ethnic origin, trade union membership, political opinions, religious or philosophical beliefs.