Keeping your research data secure

In this post we will introduce you to what you need to consider to store, share, and dispose of your research data securely.

# Introduction

The security of research data is essential to protect against data loss, unauthorised access and change, disclosure and ensure compliance with institutional, funder, data provider and legislative requirements.

In this post we will look at what you need to consider from collecting and storing your data through to sharing and disposing of data appropriately.

# Key areas of data security

Data security is important to protect highly restricted or sensitive information, for example where personal data, intellectual property, commercial interests, or national security is involved. This is commonly referred to as ‘special category data’.

## Security of special category data

You can find out more about what special category data is and your responsibilities in the resource ‘[Find out how the data protection principles apply to research](https://medium.com/my-research-essentials/find-out-how-the-data-protection-principles-apply-to-research-7b28e2d244c7)’.

Whilst adopting a proportionate risk-based approach, the entire lifecycle of the research information needs to be considered, from creation to destruction. Minimum controls for highly restricted information to remain secure include:

* authenticated access
* 2-factor authentication
* user access controls with regular review
* encryption
* up-to-date anti-virus and firewall protection
* accessing using a UoM managed device
* identified and guaranteed the location of the information

A good example of special category data is if you intend to capture audio, video or images of participants. Still and moving images and sound recordings featuring identifiable individuals contain the personal data of the participants. This means they must be processed in accordance with data protection laws. [Taking recordings of participants for research projects](http://documents.manchester.ac.uk/display.aspx?DocID=38446) is the standard operating procedure for secure handling of recordings and transcriptions.

## Physical and network security

Physical security, network security and the security of computer systems and files each need to be considered to ensure the protection of information and prevent unauthorised access, changes, disclosure or destruction of information.

The [Information Governance Office](https://www.staffnet.manchester.ac.uk/igo/) provides a review service which will be necessary if you are processing personal data and need to carry out a Data Privacy Impact Assessment (DPIA). You are likely to need to carry out a DPIA if you are using new technologies and/or cloud-based solutions, if your research data leaves the European Economic Area (EEA), or if The University of Manchester does not provide you with the required tools.

# Storing research data securely

When choosing storage options you need to consider:

* Where, when and how the data will be backed up?
* Is the data stored securely?
* Who can access it and how?
* How will you archive your data at the end of your project?
* Is your chosen storage solution appropriate for the type of data and your requirements?

## Storing personal data

You should not keep ‘Person Identifying Information’ (PII) indefinitely and should aim to anonymise it as soon as possible or follow the retention as prescribed by your funders, data providers or in line with University [Records Retention Schedule](http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=6514+).

You should, make sure you have processes for secure deletion of the data, both paper and electronic. Retention does not mean you archive after the retention period has been reached. At the end of the retention period, you will need to securely delete the person identifying information.

## Data storage solutions

All data must be stored and handled in a manner appropriate to its [security classification](http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=29971+), and the master copy of all digitally held information, regardless of its security classification, must be stored on University-approved systems.

If you intend to capture audio, video or images of participants, these must be stored as described in the [Taking recordings of participants for research projects](http://documents.manchester.ac.uk/display.aspx?DocID=38446) to ensure compliance with data protection laws.

To safeguard your data, we recommend using storage systems provided by the University, such as the [Research Data Storage (RDS)](http://ri.itservices.manchester.ac.uk/rds/%20) Service, Data Safe Haven etc.

**Please note:** University-provided Dropbox Business accounts **must only be used for sharing information, not long-term storage.** Your **P Drive should be avoided** as information is not accessible to others in your absence.

More detailed guidance and a summary table of digital storage and collaboration options are available on our [Storage and Collaboration page](https://www.library.manchester.ac.uk/using-the-library/staff/research/research-data-management/working/storage/options-for-storage-sharing-and-transfer/) and the [University Library Research Services pages](https://www.library.manchester.ac.uk/using-the-library/staff/research/research-data-management/working/storage/).

# Collaborating and sharing research data

There are further requirements and considerations where you are collaborating and sharing research data with colleagues, we will look at these below:

## Principal Investigator

A Principal Investigator (PI) should identify the UoM research data management storage solution for their projects, and document details in their [data management plan](https://www.library.manchester.ac.uk/using-the-library/staff/research/research-data-management/planning/). The PI should communicate these procedures to all group members. The procedures should ensure that the PI is able to access all data produced by the research group and must meet all applicable security requirements.

## Sharing and transferring digital research data

There are circumstances, such as fieldwork, where portable devices and media (e.g. laptops, hard drives, DVDs) may be necessary to temporarily store or transfer data. Where such exceptions exist, data should be moved as soon as possible to University-approved systems.

In addition, the University’s [Standard Operating Procedure for Information Security Classification, Ownership and Secure Information Handling](http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=29971) specifies that:

* All information must be stored and handled in a manner appropriate to its security classification, and the master copy of all digitally held information, regardless of its security classification, must be stored on University‐approved systems.
* Temporary storage of Highly Restricted or Restricted information outside of the University‐approved systems require the file, device or media to be encrypted and the device or media to be kept physically secure at all times.
* Highly Restricted information must always be encrypted, including data on University systems and with third‐party/cloud service providers.

To find out **more about different storage and collaboration options** and their characteristics, download the [Digital storage and collaboration options](https://www.library.manchester.ac.uk/using-the-library/staff/research/research-data-management/working/storage/options-for-storage-sharing-and-transfer/) guide from our webpages.

# Disposing of research data securely

At the end of your research project, you may be required to dispose of data and equipment following a suitable methodology. However, you cannot simply delete the data to destroy it.

**For example:** When you delete a file from a hard drive, it is likely to still be retrievable (even after emptying the recycle bin). Even reformatting a hard drive is not sufficient. Files need to be overwritten multiple times with random data for best chances of removal. **The only sure way to ensure data is irretrievable is to physically destroy the drive using an approved secure destruction tool.**

Data providers usually require evidence and assurance that the data has been disposed of irretrievably. There are tools such as Blancco which can be used in such cases. With regards to the RDS service, The University of Manchester have worked with 3rd party data providers to provide alternatives for more complex storage solution which ensures:

* A process is brought together as a standard operating procedure.
* Data is irrecoverable.
* Destruction of data is evidence-based.
* Hardware is destroyed in-house at end of life.
* Destruction is certified by Research IT and linked to the standard operating procedure.

## Providing evidence of disposal

Third party data providers will often ask for evidence of data disposal/destruction. This must be written up on a form normally provided by the third party, describing what, how and by who, with a signature of a witness in IT.

The evidence and completed form should be forwarded to the third-party data provider, and a return email of acceptance of the approach and destruction requested. This should be stored safely in case of an external audit.

# Summary

In this post we have introduced you to the key considerations and your responsibilities when storing, sharing and disposing of research data to ensure it stays secure.

For further support and guidance on digital data solutions you can contact [Research IT](http://www.itservices.manchester.ac.uk/research/). [Information Governance](http://www.staffnet.manchester.ac.uk/information-governance/) also provide support and guidance on data protection, records management, information security and a risk review service.

# Thank you to our contributors

This resource was created in partnership with University of Manchester’s Research IT, specifically Mary Mcderby who wrote and advised on the content.