13. Secure Storage of Data

Clear and accurate records enable researchers to demonstrate the procedures and good practice followed and strengthens the reliability of their research. They can protect researchers against allegations of misconduct, show good ethical practice or legal compliance and ensure protection against intellectual theft.

This section outlines the requirements for good records management practices in research projects conducted by staff and students at Northumbria University. Research funded by an external agent may require researchers to follow external practices dictated by the funding party.

Which records are retained?

Researchers are expected to maintain clear and accurate 'whole life' records of all the work they undertake. Records include, but are not limited to:

- Project proposals and applications for funding (including rejected)
- Evidence of any revision to original project proposals
- Project administration and management information (including staffing records, invoices, timesheets and claims etc.)
- Details of the procedures followed, risk assessments undertaken, ethics approvals
- Participant consent forms, primary data generated or collected (recordings, transcripts, databases, photographs etc.) and interim results
- Final outcomes and presentation of results (including organising any promotional events, cost of publishing etc.).

Responsibility

It is the responsibility of the Principal Investigator on any project to ensure that accurate records are maintained and securely stored for the duration of the project. This includes:

- identifying where the project is subject to the provisions of the Data Protection Act 1998 and the requirements therein. See: *Data Protection and Research Records*
- identifying how information will be collected and stored (what format below)
- using the University retention schedule (or the requirements of the project funder) to identify where information is to be retained beyond the final project output date and checking to make sure that appropriate action is taken. See: *Research Records Retention Schedule or the funding bodies requirements*

The Principal Investigator must also ensure that where there is staff involvement on the project, whether in a support or direct involvement, responsibilities are clearly defined and documented.

What format should be used?

Where possible, records should be created and stored electronically. However, the format will depend on the nature of the record itself and the reason for its existence. For example, if the record is an interview with a test subject in which personal data is shared, it could be created as an electronic sound file or as a set of hand written notes.

If the intention is to keep these in their "original" format for the duration of the project, then the storage solution could be to either copy electronic sound files to the network drive or
store handwritten notes in a filing cabinet* It might also be feasible to scan the handwritten notes and store them as electronic files.

If, however, the intention is to electronically transcribe the recorded conversation or type up the hand written notes immediately before disposing of the originals, the long-term storage solution resorts to the storage of the completed transcripts whilst also ensuring the secure disposal of the originals. The method of storage will also be determined by the content of the record. Records containing sensitive personal data or commercially sensitive information will naturally require more secure methods of storage than those which do not.

How records should be stored

Once the Principal Investigator has determined the format in which the record will be created (based upon the likely format and content), the decision on how it will be stored can be taken. Records should be stored in a manner which is "appropriate" and takes into account the balance between the need for practical access to the record with any requirement to maintain it. It should remain secure through controlled access or regular backup.

Records should be stored in a manner that identifies the content of the record quickly and easily. The same rules should be applied whether the records are stored in hard or electronic copies.

'Hard copy' records such as paper documents, tapes, photographs or removable media (memory sticks, disks etc.) should be stored and indexed in appropriate secure containers such as lockable filing cabinets, draws or shelves. Longer retention periods may require this information to be sent to the University offsite storage provider after the project completion.

'Electronic records' should be stored in logical files structures and indexed using logical file naming conventions and appropriate security measures.

What are "appropriate" security measures?

There is no single solution for secure storage of project records. Projects that involve the collection of sensitive personal data or commercially sensitive information will require more secure storage than those that do not.

The following are "appropriate", but not definitive, recommendations for securely storing records:

Projects storing records containing 'sensitive' or identifiable personal data as hard copy materials need to make sure that they are stored in a manner that will prevent unauthorised access. This can be achieved through simple measures such as:

- Locking them away in a filing cabinet or
- Ensuring that they are stored in a lockable room.

Assuming everyone remembers to lock the cabinet/room, access should be restricted to authorised members of staff. The extent and degree of security required is closely linked t the nature and sensitivity of the data, the risk from accidental loss, damage or theft, the damage that might arise from its loss and the number of potentially affected individuals. The more sensitive or risky the material the stronger the security arrangements required.

Where personal or sensitive data is held on a computer, there are a number of ways in which files can be protected. These can be as simple as:

- Applying a password to the record or the parent folder
- Limiting access to the storage area – i.e. setting permissions to allow only key individuals to see or open the folder/record
- Remembering to "lock" the PC when leaving the room – i.e. pressing "Ctrl, Alt and Delete" and selecting "Lock Computer"
- Making sure the information is backed up. If the backup is stored locally on CD, DVD or memory stick, remember to keep the device locked away securely. Data held on a removable device should be encrypted.

Collecting or removing information from the University

The management of records extends beyond the confines of the University campus. If there is a requirement to remove or collect data to or from an external site, care must be taken to protect the information. The appropriate action will be dependent upon the content and physical medium in which the information is stored.

The following are “appropriate” but not definitive recommendations for securely managing records offsite:

- Never take original material off site. Take a duplicate (even hard copy) so that if the information is lost or stolen, the original is still available.
- If collecting the information offsite, take care transfer it to the University at the earliest opportunity.
- Never leave any records unattended.
- Ensure that any personal information taken off site is anonymised. If it is lost or stolen, anyone looking at the information should not be able to identify the subjects.
- Think about the suitability of the surroundings before working. For example, if working on a train or in other public areas, do not “spread papers out” so they can be read by the person next to you.
- Where records are being collected by post (for example responses to surveys) the return envelope should be clearly marked with the University logo and marked as ‘Confidential’.

What happens to the records when the project ends?

At the end of the project, the Principal Investigator must ensure that the records are either disposed of securely or, where required, retained in accordance with the retention schedule of either the project funder or the University. See: *Research Records Retention*

Arrangements for the archiving of electronic materials should be made within the Faculty. Hard copy records can be sent to the University’s offsite storage facility. There is no requirement to retain multiple copies of the same record.

A record of archived material should be retained centrally within the faculty together with a clear indication of the length of retention. Authorised and certified destruction will then be arranged at the appropriate time.

University guidance on Data Retention

The University Retention schedule documents the minimum retention periods for Northumbria University research records.

Retention periods are independent of format and therefore can be applied to any medium whether paper or electronic. Retention periods in this document are defined as the ‘Minimum’, which mean that files may be retained for a longer period should they be required but must not be disposed of before the identified time.

Research projects sponsored by external funders may be required to follow the retention practices of the sponsor rather than those outlined in this schedule.

The research section of the University retention schedule can be found on the University website here.

The University Research Data Management Policy can be found here and additional guidance and resources can be accessed here.

For further information and advice please contact the Records and Information Manager,
duncan.james@northumbria.ac.uk