Central University Research Ethics Committee (CUREC)

Best Practice Guidance 09_Version 2.0

Title: Management of Data Collected for Research Purposes

Contents

Introduction ........................................................................................................................................ 1
Informed Consent ................................................................................................................................. 1
Safe data gathering and storage .......................................................................................................... 2
Levels of anonymisation ..................................................................................................................... 2
Retention of data ............................................................................................................................... 2
Disposal of data .................................................................................................................................. 3
Special considerations for audio / visual data .................................................................................... 3
Resources ............................................................................................................................................... 4

Introduction

This guidance has been produced to supplement the University’s Policy on the Management of Research Data and Records\(^1\) and is intended to assist staff and students whose research involves human participants, or personal or sensitive data as defined in the Data Protection Act 1998. For information about all aspects of research data management and planning please also see the University’s research data website at http://researchdata.ox.ac.uk/.

Informed Consent

Before such research starts, the participants should normally be fully informed about how their data will be managed by the researcher. It should be clear, for example, how it will be gathered/ transferred/ transcribed, who will have access to it, where it will be stored and what potential use may be made of the data (e.g. publication). Researchers should avoid making promises that may be difficult to keep, e.g. that data will only be seen by the PI, or that all data will be destroyed at the end of the project. It is likely that research data will be seen by research teams and technical/IT support, so it would be wise not to restrict who may see the data too much in the informed consent documents/ scripts unless there are strong reasons for doing so. Equally, the research data should ideally be preserved as long as possible for academic use. There is a minimum storage period of 3 years after publication according to University policy. Please see ‘Retention of data’ for further information.

\(^1\) http://researchdata.ox.ac.uk/university-of-oxford-policy-on-the-management-of-research-data-and-records/
For further advice on informed consent, including recommended templates, please see http://www.admin.ox.ac.uk/curec/resources/informed-consent/.

Safe data gathering and storage

While gathering data in the field, mobile devices containing University data should be protected by whole disc encryption. Third party online cloud storage like Google Drive, Dropbox and OneDrive is not generally an appropriate place to store research data (especially sensitive data) unless all data is encrypted. Please contact researchdata@ox.ac.uk for advice on alternatives.

Personal and sensitive data must be transferred and then stored as safely and securely as possible at the Principal Investigator’s University department or faculty, e.g. using encrypted laptops, encrypted USB sticks, encrypted files in departmental storage systems (e.g. SharePoint) or locked filing cabinets.

Researchers must consider the security of the re-transmission of all data if shared with the participant for the purpose of checking the accuracy of a recorded statement. Again, the researchdata@ox.ac.uk team can advise on this.

Plans for your research should include a framework that indicates how this will be achieved during and after the research project. Please see http://researchdata.ox.ac.uk/home/managing-your-data-at-oxford/storage-and-backup/ for further information.

Levels of anonymisation

In general, data should be managed and used in such a way as to protect the confidentiality of the research participants. This is of particular importance if the data involve personal interviews or results from standardised cognitive tests, where the participant would not want results disclosed to others. Anonymisation is one option (the other is restricting access to data) and should be considered in relation to the demands of the project and the expectations of participants. Some base level anonymisation is advised in the handling of data files as well.

For example, it is good practice in general to use a code number to label all paperwork, physical media (e.g. audio recordings, CDs) and computerised records (even discussion via email), with a key giving identities stored separately. The benefits and drawbacks of anonymisation regarding the security and quality of your data need to be considered. Contact the research data team (researchdata@ox.ac.uk) for more advice about data anonymisation and access control.

Retention of data

Research data and records should be retained for as long as they are of continuing value to the researcher and the wider research community, and as long as specified by research funder, patent law, legislative and other regulatory requirements.

The minimum retention period for research data and records is three years after
publication or public release of the work of the research according to University policy, though funders and regulators may require longer retention periods.

According to the UK Data Protection Act’s exemptions for researchers, there is not currently a maximum data storage limit or an expectation that data must be destroyed after a set time. Funders, of course, will often have their own requirements.

In many instances, researchers will resolve to retain research data and records for a longer period than the minimum requirement. Data archives and institutional repositories (such as ORA-data at Oxford) are working to address this development. As different regulations apply to how long researchers are required to store records after the completion of research, researchers should look into what repositories might be available to them as a result of their divisional, departmental or institutional affiliations. Researchers must keep records for the longest applicable period of time or include them as part of a dataset if they are deposited into an archive.

Practical considerations of storage space for data during a project will need to be considered. Expectations and requirements to preserve the data for a long time after the project – when appropriate - will also needed to be planned. This may include instances where researchers wish to reuse their own data for subsequent studies or share it with other researchers after preservation. This situation should be anticipated, and addressed in the original study’s information sheet and consent form.

Disposal of data

If there are strong reasons why research records need to be destroyed instead of stored and preserved securely, researchers should include additional stages clearly designed to protect their participants’ confidentiality throughout the process rather than as a set of ‘project end’ measures. Paper records should be shredded. Records stored on a computer hard drive should be erased using commercial software applications designed to remove all data from the storage device. Contact the research data team (researchdata@ox.ac.uk) for more advice about erasing electronic records. For data stored on USB drives or recorded data on tapes, CDs, or DVDs, the storage devices should be physically destroyed or made unreadable. Local IT support staff periodically hold hard drive destruction ‘events’, which researchers could take advantage of. Researchers should keep records stating what records were destroyed, and when and how they did so.¹

Special considerations for audio / visual data

Increasingly researchers are in a position to gather data using mixed media that adds new dimensions to the potential for analysis. The value of this needs to be recognised. Where data consist of recordings of individuals, it is especially important to gain explicit consent for audio recording/ video recording/ photography in general, and to gain explicit consent in case the participants are still recognisable (e.g. faces, voices).

The material recorded may be such that the participant is happy to waive the requirement for confidentiality, and agree that the researcher is free to use the material in any way he/she chooses, e.g. in public lectures.

Where there is any potential sensitivity of content (e.g. the participant may express views

¹ Based on advice from http://www.virginia.edu/vpr/irb/sbs/resources_guide_data_retention.html
that are private, or demonstrate incompetence in a task), then it is incumbent on the researcher to take extra safeguards. For the majority of projects, points a) and b) below are the most important ones:

a) Informed consent must be in place, which also complies with any data policies of research collaborators (if applicable). The participant information sheet should include that the material will be seen only by members of the research team and other academics (not by members of the public).

b) The relevant recordings should be kept in secure, long-term digital storage, or, for hard copies, in a locked filing cabinet.

In addition, the following safeguards will need to be considered if appropriate:

c) Participants should clarify during recordings any sections that are ‘off the record’.

d) Researchers undertake to vet access to data by others.

e) Researchers should be sensitive to the (rare) possibility of recordings being ‘lost’ after being archived, and only discovered years later after the researcher who collected the data has disappeared. The researcher should make a plan for the storage and ultimate disposal of the material. Any material that is archived must be labelled as confidential, with the name and contact details of the researcher attached.

f) Special steps will be taken to ensure data is migrated off devices (and fully deleted from them) to secure encrypted storage immediately.

g) Recordings of children raise two additional ethical issues:

i.) Researchers should be aware that parents and teachers may be concerned that even innocuous recordings of children could be misused, so care should be taken to stress the protections researchers are placing around the data balanced against the benefits of their participation, and the integrity of their research project. Point (b) should be adhered to even when the content of the recording is not apparently sensitive.

ii.) With the passage of time, a child participant may no longer agree to their data being retained. This is unlikely to be a realistic concern except where an adult has given permission for a video of their child to be made more widely available, e.g. as an illustrative example in a lecture. For ongoing studies, once child participants have reached an age where they can give their own consent, then this should be sought before making the materials available to those outside the research group.

Resources

Further advice on research data management is available from the Oxford Research Data website at http://researchdata.ox.ac.uk/, including advice on:

- The University Policy on research data management
- The University Policy on Data Protection
- Working with data, including
  - data management planning
  - ethical issues and data protection, and
  - data backup, storage and security
• **Sharing Data**
• **Tools, services and training**

Please ensure you have robust research data management plans in place demonstrating a consideration of these points before applying for research ethics review.