Classification, storage and retention of research project data

1. Purpose

The University's *CoP for Professional Integrity in the Conduct of Research* requires that research data (documentation and records) must be kept for a minimum (or default) period of ten years after the end of any particular study. In addition, many research funders, collaborators or commissioning organisations are likely to have requirements that exceed the University minimum. It is also expected that researchers will wish to retain information securely beyond the ten year period. The purpose of this document is to instruct staff and students in the appropriate classification, storage and retention of research project data to ensure that it remains secure, viable and accessible.

The University's retention and disposal schedule provides more detailed information on the requirements for specific types of documentation (see pages 1 to 10). This can be accessed at:

https://secure.ulster.ac.uk/isd/policies/Policies/Approved/Records%20Retention%20and%20Disposal%20Schedule%20Draft%2020120604.pdf

Staff and students should also refer to the University publication/staff information handbook, *Protecting University Information* for further guidance:

http://ulster.ac.uk/__data/assets/pdf_file/0004/2776/staff-handbook.pdf

In particular, attention must be paid to the classification of data and documentation, restrictions on storage and electronic transmission and the University's responsibilities under the Data Protection Act and Freedom of Information Act. The requirements of the Human Tissue Act, IRMER and other relevant legislation also hold implications for the University and individual researchers and must be observed.

2. Scope

This procedure applies to all staff and students of the University who require to retain research records or documentation.

3. Classification and marking of research project data

3.1.1 The University's policy on protecting information has three classifications or markings: open, protect and control.

3.1.2 All research project data must be classified and marked as "protect" as a minimum standard; sensitive personal data or data which might lead to significant personal distress if disclosed should additionally be classified and marked as "control".

3.1.3 CIs/PIs must ensure that all research project data is appropriately marked, in line with the guidance provided by the University in the staff information handbook, *Protecting University Information*:

http://ulster.ac.uk/__data/assets/pdf_file/0004/2776/staff-handbook.pdf

3.2 Storing hard copy research project data and documentation

3.2.1 All hard-copy research project data and documentation must be stored in compliance with the University's policies and guidance and must be classified and marked appropriately.

3.2.2 All original hard-copy project data must be held securely and on University premises; irreplaceable data (eg, consent forms, interview notes, returned questionnaires) and data from which individuals might be identified (eg contact details, medical records) must be kept in a locked drawer or equivalent when not in use and should not be removed from University premises.

3.2.3 Administrative or supporting documentation (eg, letters of approval, original protocol/application form, updates and amendments) should be held in a project folder in a secure location; master files which include participant/sample and other coding information must be treated as project data (see 5.2.1 above) and kept in a locked drawer when not in use.

3.2.4 All hard-copy documentation should be stored in a manner which facilitates legitimate use and access; file names should be logical and relevant; version control is critical and it should be clear which version of any document is the most recent or currently approved for use.

3.2.5 For details of the documents that must be retained for studies regulated under the Human Tissue Act and/or under IRMER, please refer to appendices 1 and 2 to this document.

3.3 Storing electronic research project data

3.3.1 All electronic research project data must be stored in compliance with the University's policies and guidance and must be classified and marked appropriately.

3.3.2 All original, irreplaceable electronic project data and electronic data from which individuals might be identified must be stored on University-supported media, preferably appropriate centrally-allocated secure server space or similar; such data must never be stored on portable devices or temporary storage media.

3.3.3 All other electronic project data must be held on appropriate centrally-allocated secure server space which is accessible to members of the project team; such data must not be held on personal or portable devices unless these are encrypted in line with University requirements and except when this is necessary for the purposes of working off-site; amended documents must be returned to the appropriate University-maintained shared space when the work has been completed.

3.3.4 Under no circumstances should original, irreplaceable data or sensitive personal data be stored using cloud storage services as this can place data outside UK and EU legal control.

3.3.5 All electronic data should be stored in a manner which facilitates legitimate use and access; file names should be logical and relevant; version control is critical and it should be clear which version of any document is the most recent or currently approved for use.

3.4 Controlling access to research project data

3.4.1 Research project data should be stored as indicated above and should be protected by password, encryption (for electronic data) or lock and key (hard copy).

3.4.2 Research project data, whether electronic or hard-copy, should be accessible only to those people who have a legitimate purpose, including members of the project team, internal and external auditors and representatives of regulatory bodies.

3.4.3 Members of staff, students and people external to the University who do not fall into the categories above should not be given access to research project data without good reason and/or prior permission.

3.4.4 Research project data must be maintained in such a way that any person with a legitimate purpose can access it at any time and without giving notice.

3.4.5 Requests for access to research data by parties not listed under 5.4.2 above must be directed through the CI in the first instance.

3.5 Archiving and disposal of research project data

3.5.1 All research project data, following the end of the ten year data retention default period, can be submitted to the University Archive for continued secure storage or may be retained by the researcher if preferred.

3.5.2 Applications for archiving research data must be made in line with the process described in the archiving procedure, available at:

http://research.ulster.ac.uk/rg/1010%20Archiving.pdf

3.5.3 Research project data that is no longer required may be destroyed, subject to the demands of the publication cycle, continuing or follow-on projects or the requirements of any funder, sponsor or publisher.

3.6 Handling personal information and the Data Protection Act 1998 (the DPA)

3.6.1 The University is bound by, and all staff and students are required to be aware of and to adhere to the provisions of, the DPA. Guidance on the DPA and the retention, disposal and transmission of personal information is available in the University's Data Protection Policy (the Policy) which is available online at:

http://www.ulster.ac.uk/secretary/policyimplementation/dataprotection/data_protection_policy.pdf

3.6.2 Staff and students are required to abide by the Policy. Any alleged breaches of the DPA by staff and/or students will be fully investigated and may result in disciplinary action and may, in some instances, be considered gross misconduct. ***It is compulsory for all staff to complete the University's data protection training programme.***

3.6.3 The primary function of the DPA is to ensure that an individual's personal information is used only as agreed with that individual and is not used for any other purpose, including forward transmission to a third party.

3.6.4 The DPA states that "personal data processed for any purpose or purposes shall not be kept for any longer than is necessary for that purpose or those purposes".

3.6.5 The following principles should be adopted when handling personal information:

- data should be anonymised at the point of collection where possible;
- all other data, unless there is a specific reason for maintaining an identifying link, should be anonymised as soon as possible after collection;
- data that cannot be anonymised must be held securely and in confidence, with coded access as appropriate, for a pre-set period of time which is subject to the consent of the individual concerned and the needs of the study or potential future requirements (including, for example, those of the Human Tissue Act);
- anonymous, raw data should be transcribed or transferred for analysis as quickly as possible after collection;
- once transcribed or transferred, the data should be stored securely in condensed form;
- as soon as transcription and validity have been assured to the satisfaction of the Chief Investigator, the raw data may be destroyed, *subject to the requirements of any contract, funding body or other interested party*, although there is no absolute requirement relating to this;
- condensed or interim data must be handled and stored as indicated in the *CoP*;
- interim data, all other related materials and results will remain the responsibility of the researcher or other appropriate individual until it can be demonstrated that: the project has been completed to the satisfaction of the funder/sponsor, any publications have been finalised to the satisfaction of all concerned and/or until any queries relating to the project have been addressed; and
- all retained information relating to the project should then be transferred to a secure local repository (data store or similar), central University archive or specified data bank for the remaining period specified in the *CoP* or in any contract, funding or sponsorship agreement.

3.7 Breach of the DPA

3.7.1 Any unauthorised or unlawful processing, accidental loss or destruction of, or damage to, personal information held at the University in both electronic and hard copy format will constitute a breach of the DPA. Any such breaches will be reported to the Information Commissioner's Office who, since April 2010, has the power to impose enforcement notices and monetary penalties of up to £500,000 for the most serious incidents.

3.7.2 Any breaches must be reported to the University Secretary in line with the procedures set out in the University's Data Protection Policy which is available online at:

http://www.ulster.ac.uk/secretary/policyimplementation/dataprotection/data_protection_policy.pdf

3.8 Handling personal information and the Freedom of Information Act

3.8.1 It must be noted that the Freedom of Information Act 2000 (FOIA) gives the public the right of access to information held by public authorities, including Universities.

3.8.2 Information is made available on request unless there are justifiable reasons for withholding it (known as exemptions).

3.8.3 The University Secretary is authorised ultimately to determine what information should be disclosed and what, if any, exemptions might apply.

3.8.4 All research-related information must be maintained and stored in such a way that any disclosure required under the FOIA will not bring the University into disrepute.

4. References

University of Ulster CoP for Professional Integrity in the Conduct of Research

University of Ulster Policy on Research using Human Tissue

University of Ulster Human Tissue Standard Operating Procedures

http://research.ulster.ac.uk/rg/humantissue.html

University of Ulster Research Governance Policy and Procedures and forms

University of Ulster Research Ethics Committee Terms of Reference

http://research.ulster.ac.uk/office/rofficeeg.html

ISD documentation

Data Protection Act

Freedom of Information Act

Archiving SOP/Procedure

Appendix 1

Documents to be retained for studies regulated under the Human Tissue Act 2004 (Cat D)

- Final approved UREC application (RG1a) and associated documents (RG2, RG3, protocol, consent form, information sheet, questionnaires and similar)
- RG1d appropriately completed
- Letter of approval from UREC and associated documentation (copy of CI undertaking, indemnity statement)
- All study consent forms, appropriately completed
- All participant screening forms, food diaries, questionnaires and similar appropriately completed
- Freezer map indicating location of samples
- All adverse event reports
- Amendments
- CVs
- Training record for any training events that are relevant to conducting the study

Appendix 2

Documents to be retained for studies regulated under IRMER (DXA)

- Final approved IRAS application including fully executed (by MPE) non-NHS SSI and associated documents (RG2, RG3, protocol, consent form, information sheet, questionnaires and similar)
- Letter of approval from ORECNI
- Sponsor letter, indemnity statement, copy of CI undertaking
- Copy of practitioner justification guidelines
- All participant screening forms
- All bone densitometry referral and confirmation forms, appropriately completed
- All DXA consent forms for all scans, appropriately completed
- All study consent forms (if different to above), appropriately completed
- All adverse event reports
- CVs
- Training record for any training events that are relevant to conducting the study