## GUIDANCE NOTES FOR INVESTIGATORS

# Data Collection and Storage

The Ethics Review Sub-Committee has approved the following guidance for investigators regarding data collection and storage.

## 1. Data Collection

It is the responsibility of investigators to ensure that they collect and store data in accordance with relevant legislation. Investigators should ensure that any data collected, stored and archived also meets the requirements of their funder.

Investigators must ensure that they **only collect data which is necessary** for the study. Investigators must think carefully about the design of their studies/data collection methods to ensure that only relevant information is collected.

Investigators should consider what verification procedures are required to ensure that accurate data is collected and recorded.

Participants must be provided with details explaining:

- Who will own the data created in the course of the research.
- Who will have access to the data.
- The length of time for which data will be retained.
- What the data will be used for.
- Whether and where the data will be archived.

Funders may require a data management plan (DMP) to be submitted with the funding proposals. The recommended tool for the creation of a DMP is DMPOnline..

## 2. Identifiable Personal Information

Identifiable personal information is subject to Data Protection Legislation. Data processing must be **lawful**, **fair** and **transparent**. Being fair with research participants includes respecting their rights and ensuring that personal data is used in line with their expectations and consent.

Personal data is data relating to living people from which they can be identified (directly or indirectly). This is very broadly defined, and includes data containing names, postcodes, photos/videos, email addresses, bank details, social networking posts, job title, GPS location data and unique online identifiers including IP addresses, etc. See: *https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr*

Particularly sensitive personal data - such as data about health, political opinions, religious beliefs, or genetic or biometric data that is uniquely identifying - are classed as special categories of personal data and require additional protection.

Personal information must only be retained for as long as it is required for the study.

See the Guidance Note on Data Protection Requirements and the websites on GDPR: Implications for Research and Loughborough University's Data Protection Policy.

## 3. Anonymisation

All data should be encoded or anonymised as far as is possible and consistent with the needs of the study. However, the use of pseudonyms is **not** classed as anonymisation under data protection legislation so pseudonymized data would still be considered personal information.

In most studies, participants should be assigned a reference number or code as early as possible and data should be stored against this number/code rather than against the names of participants. Investigators may wish to maintain separate lists of people who have taken part in their research, but steps should be taken to ensure it is not possible to relate a particular set of data back to any given participant. Coding details (e.g. Codebook) should be stored separately from the anonymous data.

If data is not being anonymised and participants will be identified within the study outputs, e.g. through case studies, attributed quotations or photographs/videos, they must give explicit consent to be identifiable in the Informed Consent Form.

## 4. Storage

Data should be stored on the University's provided systems and services (e.g. OneDrive) so that it is retained safely with appropriate back up and contingency plans in the event of loss, damage or unauthorised access to the data. It is important that data is maintained in its original form or non-editable digital format, e.g., pdf, as a necessary precaution, particularly if published results are challenged by others.

Hard copies of documents should be stored in their original form in locked filing cabinets in a secure location on campus or as scanned copies on the University's provided systems and services (e.g. OneDrive). For studies conducted overseas hard copies must be stored in a secure location in accordance with local approvals.

**Staff and postgraduate research students (PGRs)** should retain data subject to periodic review (normally 10 years from the point of last access) or archive data to the University's Research Repository, see below. If a PGR or staff member leaves, they should transfer the data into the ownership of the most appropriate staff member (e.g. a PhD supervisor).

**Undergraduate and postgraduate taught students** should delete their data after they have fully completed (including scope for appeal) any assignment for which the data will be used. However, if the data is to be of value for a larger/ongoing project or is being retained by the University for future research, they should transfer the data into the ownership of the most appropriate staff member (e.g. a project supervisor).

## 5. Archiving or Retention for Future Research

If investigators intend to add data to the University's Research Repository, or to a data archive in compliance with funder policies (e.g the UK Data Archive), participants should be informed of this at the study's outset and should give consent. Investigators should note that many journals now expect published data to be made available through a repository.

In addition, PhD thesis, which may include data, are deposited to the Research Repository on submission.

For further details please see guidance on Research Data Archiving and the Loughborough Research Data Management Policy.

If data is being retained for use in future research the participant should be informed of this and should give consent. Please see the University's Open Research Position statement.

## 6. External Data Sharing

If data is being shared with external study partners, e.g. investigators at other institutions, investigators must ensure that they use a safe method for transferring this data. Sending data by email is not considered secure. Participants must be aware that data is being shared with external partners. Identifiable personal information must not be shared beyond the terms of the consent given by participants.

Further details on secure methods for sharing data can be obtained from IT Services.

## 7. Withdrawal of data

All participants should be given the opportunity to request that their data be destroyed/withdrawn from a research project. In all cases, investigators should aim to comply with such a request, but compliance may not always be possible, for example where:

- Final results have already been published.
- An individual's data is no longer identifiable (because of encoding/anonymity etc).
- An individual's data cannot be extracted from cohort analysis.

Participants should be advised of the latest opportunity for withdrawing their data. If it is not possible to withdraw an individual's data for any reason, the investigator is responsible for explaining this to the participant.

## 8. Further Information

This guidance is not intended to be an exhaustive list of considerations in relation to the collection and storage of data for research projects. However, it is hoped that these guidelines will encourage researchers to adopt best practice and familiarise themselves with the relevant legislation.

The following websites may also be of interest:

- DMPOnline
- Loughborough University IT Services
- Loughborough University Information Governance
- Loughborough University Data Management Plans
- Loughborough University Research Data Management Policy
- Loughborough University Data Archiving
- Loughborough University Data Protection Policy
- Loughborough University: GDPR: Implications for Research
- UK Policy Framework for Health and Social Care Research
- Market Research Society Code of Conduct
- Medical Research Council
- Information Commissioner's Office
- Medical Research Council online training course on Research Data and Confidentiality
- UK Data Archive