GUIDANCE ON DATA PROTECTION, CONFIDENTIALITY, AND RECORDS MANAGEMENT IN RESEARCH

The legal framework for processing personal data is the **General Data Protection Regulation (GDPR)** and associated UK legislation (the Data Protection Act 2018)[1]. Compliance with the GDPR is a legal requirement. In the event of breaches of data law, institutions are liable for investigations, substantial fines, adverse publicity and civil or criminal liability. Enforcement action may be taken by the Information Commissioner's Office I.3(n)--rm

The University primarily processes personal data for research purposes in relation to its **public tasks** and **legitimate interests**. These legal bases for processing[5] are regularly

GDPR - Key points to consider

- Participants should be fully informed about the use of their personal information and researchers must respect participants' expectations of confidence and privacy. The principle of 'data minimisation' (taking the least personal data necessary) should apply at all times.

- Personal data cannot be used freely for further research if this research is not covered by the participants' original consent (usually detailed in your participant Information Sheet and consent form).

- You cannot collect **sensitive personal data (Special Category Data)** without explicit consent. Participants will need to know how their data will be kept securely and eventually destroyed or archived. Data in this category are those that relate to:

  - x race;
  - x ethnic origin;
  - x politics;
  - x religious or philosophical beliefs;
  - x trade union membership;
  - x genetics (DNA);
  - x biometrics (where used for ID purposes);
  - x health;
  - x sex life; or sexual orientation

  Data relating to criminal convictions and offences may be processed only under the control of official authority or when authorised by law.

  Please also see the note about Special Category Data below (iv).

- Data Protection Impact Assessments (supported by the Data Protection Officer - dpo@sussex.ac.uk) should be carried out for any project likely to pose a high risk to the rights and freedoms of individuals.

- Data must be kept securely. You need to discuss the arrangement with your School to ensure personal information provid2(he c-12.3(2(hns)-8(u8(bgi)3.1(ghm)-24 I)2.3-6.3(a)-12o.-8(houl)-8.9(d b-8(o s)-8(ee)-12.2(

i. Data Collection for Screening Purposes

In some studies personal data is collected from people for screening purposes (to ascertain whether they are eligible to participate in the study) but it does not contribute to the study if they are excluded as a result of the screening. Please ensure that you either obtain specific consent for the collection and use of personal data for the purposes of screening (using the standard sentence relating to the GDPR in the consent form) or ensure that data provided is destroyed immediately once a participant leaves the study (and that you inform participants that you will be doing this in the information provided prior to screening).

ii. Confidentiality

Confidential participant information is restricted and should not be disclosed beyond the study team. The Common Law Duty of Confidentiality[7] is a key attribute of research practice which arises when a direct assurance of confidentiality is given by a researcher to a participant. A duty of confidence may also arise naturally when material of a sensitive or private nature is exchanged in a confidential context. Here a participant will have every right to expect that their information will remain confidential even if no direct assurance has been given. **NOTE: Researchers should generally assume that the personal information of participants is confidential especially if it touches on private or sensitive matters. Any exceptions to this should be subject to specific participant consent. Failure to follow these standards may be considered a breach of the University's** Code of Practice for Research [8]**.**

iii. Security of Data

Researchers have a legal duty to make sure that confidential information stays secure. Anonymisation is often the best technique. Proper anonymisation ensures that privacy is protected and that sensitive data cannot be directly associated with any specific individual. Sometimes it may be appropriate for a participant to remain personally associated with their contribution. It might be right in terms of the data and of the study that information is not anonymised. In these cases the consent of participants should be secured. If confidential information needs to be disclosed to translators, transcribers, auditors or anyone else then this should be made clear to participants at the outset and a confidentiality agreement should be signed by the company providing this service. If the research will lead to the public disclosure of

v. Data and Records Management R esponsibilities

In addition to research data, consent forms and administrative records also need to be properly managed throughout the study. Signed consent forms are especially important and are an essential source of evidence in claims of harm resulting from participation. They must remain secure and accessible at all times. It is recommended that the study consent form and information sheet be printed back to back on the same sheet of paper. Participants should always be given their own copy of the information sheet to keep.

It is essential to retain an adequate record of the study's progress for audit and review and to manage ongoing liabilities. At the end of the study the following records should be collected together and stored securely for an appropriate period as indicated in the University's Master Records Retention Schedule[14] :

- A copy of the research protocol;
- A copy of the application for ethical approval along with related correspondence;
- Details of research participants including names and, as appropriate, addresses, dates of birth and other relevant details[15];
- A copy of the code which links participants' names to research data/results as appropriate;
- All Data Protection Impact Assessments undertaken before, during and after the research
- All records relating to unexpected events that arose during the research;
- Copies of research data/results;
- Copies of research publications.

The Principal Investigator is formally responsible for making proper arrangements for the ongoing storage of all study information. Storage of both physical and electronic information must be secure. The appropriate period for which study information should be retained may vary. It will depend on the nature of the study and on funder or sponsor requirements. On completion of the research, all remaining personal data should be systematically deleted (digital) or safely destroyed (hard copy).

For original research, **anonymised data** [16]

Occasionally research brings to light information about a participant which could affect the welfare of others, or the participant. For instance, an interviewee might reveal professional misconduct or a risk to public health. In these cases the need for

approval by an NHS research ethics committee after securing University Sponsorship[20].

Wherever possible, the use of anonymised or pseudo-anonymised data only within the University (with the NHS partner holding the ‘key’ to the personal identifiers) is the preferred way of working to protect the interests of all parties. Researchers should p

vulnerable individuals. Where appropriate, letters to parents, teachers and medical staff should be provided. Research involving adults (aged 16 or over) lacking the capacity to consent is governed by sections 30-34 of the

which arise from this type of research and how to address these in a research ethics application.

iv. Deception or subterfuge

Normally deception is to be avoided unless the research topic explicitly demands this to ensure that the appropriate data are collected. In this case, you will need to clearly justify using this type of research in your ethics application. In this type of research, it is particularly important to safeguard the anonymity of participants, and where ever possible, informed consent should be sought post-hoc (British Sociological Association). See also the relevant sections of the British Psychological Society Code of Ethics and Conduct.

Research Governance Office
Updated May 2018

Acknowledgements: King's College London, University of Oxford

Appendix A: Data Protection Principles

The General Data Protection Regulations require that the University and all those who work within it (staff and students who act as 'data processors') process all personal data in accordance with the six Data Protection Principles.

When processing personal information data must be:

1. **Lawful, fair and transparent**
   Lawful: processing must meet the tests described in the legislation
   Fair: what is processed must match up with how it has been described
   Transparency: tell the subject what the processing is for

2. **Limited in Purpose**
   Personal data can only be obtained for "specified, explicit and legitimate purposes"

3. **Minimised for processes purposes**
   Data collected on a subject should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed"

4. **Accurate**
   Data must be "accurate and, where necessary, kept up to date"

5. **Limited in storage**
   The regulator expects personal data is "kept in a form which permits identification of data subjects for no longer than is necessary". In summary, data no longer required is removed

6. **Subject to appropriate storage arrangements**
   The legislation requires processors to handle data "in a manner that ensures appropriate security of the personal data", including protection against unauthorised or unlawful processing and accidental loss, destruction or damage

Further information about Data Protection and the University can be found on the University's Planning, Governance and Compliance web pages - http://www.sussex.ac.uk/ogs/policies/information/gdpr

Further resources

Information Commissioner's Office (ICO) -