GUIDANCE NOTES FOR INVESTIGATORS

Data Protection Requirements

The Ethics Review Sub-Committee has approved the following guidance for investigators regarding compliance with 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.

1. What Data to Collect?

Data Protection Legislation states that personal data should be relevant/not excessive and accurate.

- Investigators should think carefully about the design of their studies/data collection methods to ensure that only relevant information is collected. For example, the generic Health Screen Questionnaire should be carefully **customised** for each study to ensure that only relevant questions are included. Other data collection instruments should be designed to ensure that only questions **relevant to the study** at hand are included.
- Investigators should consider what verification procedures are required to ensure that accurate data is collected and recorded.

2. Data Protection Notices

Transparency will be addressed at the institutional level in privacy notices but should also be addressed at project level. The materials you provide are often where participants get their understanding of what will be done with their personal data, so you need to be clear and transparent in the detail you give. Participants should understand the research process. You need to explain how data is used in research, who will see it, and how long it will be retained for. Explain how their privacy will be protected.

The following information, regarding processing of personal data should be included in Participant Information Sheets and/or Informed Consent Forms:

- What personal data or sensitive personal data will be collected and stored.
- What you intend to do with the personal data or sensitive personal data.
- How (format) and where (location) the personal data will be stored.
- Who will have access to the personal data (in some cases this should include whether personal data will be transferred outside the EU).
- What security measures will be in place to protect against unauthorised access.
- Details of any coding/anonymity to maintain participant confidentiality.
- If appropriate, how long the data will be stored and whether/where it will be archived for future research.

- How the data will be used in publication/outputs (e.g. whether individuals will be identifiable).
- What type of outputs will be generated using the data (e.g. reports, journal publications, conference papers etc).

3. Personal Data and Sensitive Personal Data

The General Data Protection Regulation (GDPR) applies to any 'personal data' processed by organisations in the EU, and personal data of people in the EU that is processed anywhere.

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*

It even includes data that has been pseudonymised if this can still be used to identify individuals (but not data that has been anonymised in line with the ICO code of practice)*, and covers data that is either automatically generated or manually collated.

> ***Data protection law does not apply to data rendered anonymous in such a way that the data subject is no longer identifiable. There are strict guidelines in place determining whether or not data is truly anonymous.***

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. Sensitive personal data is described in *article 9* (pg 38).

All health related personal data, including health screen questionnaires, are classified as sensitive personal data as well as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership; and the processing of genetic data or biometric data for the purpose of uniquely identifying a person; data concerning health or data concerning sex life or sexual orientation.

4. Lawful basis for processing personal data

Data Protection legislation sets out that all processing of personal data must have a legal basis in order to be lawful e.g. a legal reason for the processing. Individuals have the right to be informed about the data we hold, why we hold it and on what legal basis we are processing it. If it would be possible to undertake your research without processing personal data then your intended legal basis will not be valid.

There are six lawful bases and the appropriate one for publicly funded university research is likely to be the fact that processing is necessary to perform a **'task in the public interest'**. This assures research participants that the organisation is credible and using their personal data for public good. Commercially funded research is most likely to be carried out under the 'legitimate interest' legal basis.

You must include a statement confirming the legal basis for processing personal data in the study's participant information sheet.

Where special categories of sensitive personal data are processed, such as health data, an additional condition is needed. This is likely to be 'necessary for scientific research in accordance with safeguards'. Safeguards are processes and procedures that form accepted good practice for scientific research using personal data such as ethical approval, only processing personal data that's necessary (data minimisation), and anonymising or pseudonymising where possible.

Data should be held securely with an appropriate level of protection, and those handling the data should be aware of the importance of confidentiality.

4.1 Data Protection Impact Assessment

If your study involves a high risk to personal data you should complete a Data Protection Impact Assessment (DPIA). A DPIA is a key procedure required, in certain circumstances, by data protection legislation. A DPIA must be carried out where any processing is likely to result in a high risk to individuals' privacy interests.

4.2 Legitimate Interest Assessment

If you are using Legitimate Interest as the legal basis for processing personal information for commercially funded activity you must complete the Legitimate Interest Assessment. A copy is not required with the ethics review submission but must be retained for the length of the project. Please see details below:https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/

5. Consent

The GDPR has created some confusion around consent. Consent can be understood in two different ways: as one of the six lawful bases under GDPR (this is consent as the lawful basis for processing personal data); and as consent to take part in a research project because of ethical or other legal requirements.

Under GDPR if you are using 'task in the public interest' as the lawful basis plus the research condition for special categories of personal data, you do *not* need to meet the 'consent' requirements of GDPR, such as getting reconsent from participants every two years.

However, you will still need to seek informed consent from participants to take part in your research project. This is for ethical or other legal reasons, such as disclosing confidential information in line with the common law of confidentiality. Consent to participate in research can give participants control over how their data are used.

So participants have dual assurance: the GDPR 'task in the public interest' reassures them that the organisation processes personal data for the public good, and the existing systems by which they consent to participate give them control over how their data is used.

For *personal* data an adequate Data Privacy Notice (within the Participant Information Sheet) accompanied by a signed Informed Consent Form which includes a statement to the effect of "I have read the Participant Information Sheet" should suffice. However, for ***sensitive*** personal data **explicit** consent should be obtained. Therefore, investigators are advised to include a specific statement on the Informed Consent Form (which participants will sign) regarding the collection, storage, use etc of *sensitive* personal data.

Further assistance:

Further information is available on the University's dedicated web pages:

http://www.lboro.ac.uk/admin/ar/policy/dpact/

http://www.lboro.ac.uk/services/registry/information-governance/

Further details:

Information Commissioners Office: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Health Research Authority: https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-guidance/

UKRI: https://www.ukri.org/who-we-are/policies-standards-and-data/gdpr-and-research-an-overview-for-researchers/

Medical Research Council on-line training: https://byglearning.com/mrcrsc-lms/course/index.php?categoryid=1