UNIVERSITY OF SUSSEX

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 (ICO).

The regulation apples to the '**processing**'[2] of '**personal data'** which is defined as 'any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.
(a) from those data, or
(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller[3], and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.'

Processing is broadly defined as obtaining, using, maintaining or holding personal information Fully anonymised information is not personal because it does not identify anybody individually[4].

Under the GDPR data subjects have certain guaranteed rights in relation to the processing of their information that should be ***fair, lawful and transparent*** . This includes a right of access and in certain situations the right to prevent further data processing.

All research with human participants are likely to process personal data at some stage and all researchers are required to comply with the GDPR. Researchers should be fully aware of the requirements of the GDPR and the six data protection principles (see Appendix A below).

---

[1] https://www.gov.uk/government/collections/data-protection-act-2018
[2] 'Processing covers a wide range of operations performed on personal data, including by manual or automated means. It includes the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data.' https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_en
[3] 'Data controller' means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed. 'Data processor', in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/
[4] 'Anonymisation is the process of turning data into a form which does not identify individuals and where identification is not likely to take place.' https://ico.org.uk/for-organisations/guide-to-data-protection/anonymisation/

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 reviewed and balanced against individual rights and freedoms. Consent is relied on, as a legal basis for processing from participants of research. The form of consent that is needed from them, will depend on the type of personal information gathered and the context in which it is taking place.

The University has updated the existing generic university templates for consent form and information sheets to assist researchers in achieving the necessary standards for data management:
http://www.sussex.ac.uk/staff/research/governance/apply .

All University researchers are also required to understand and follow the *Code of Practice for Research*.[6]

[5] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

[6] https://www.sussex.ac.uk/webteam/gateway/file.php?name=code-of-practice-for-research-june-2018.pdf&site=377. In June 2018 Council approved updates that reflected the GDPR and requirements for researchers to report data breaches.

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:

  - race;
  - ethnic origin;
  - politics;
  - religious or philosophical beliefs;
  - trade union membership;
  - genetics (DNA);
  - biometrics (where used for ID purposes);
  - health;
  - 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 provided by participants (in paper form) is handled properly. Questions about appropriate University digital file storage should be directed to IT Services (http://www.sussex.ac.uk/its/services/networkandstorage/filestorage /).

STUDENTS PLEASE NOTE: You must ensure that your **supervisor** knows exactly what you are doing with the research data. ***Your supervisor has overall responsibility for ensuring that personal information supplied by participants is handled appropriately***.

- Data should not be transferred outside the European Economic Area (EEA) without formal arrangements to ensure that participants' rights are protected. Formal arrangements include formal contracts signed by authorised officials that are drawn up between the University of Sussex and any third parties who are transferring the data and applying appropriate technical and procedural safeguards.

- The ethical approval that you are applying for is **specific** to the research project that you have outlined in this application, and the consent given by participants is only for the purposes outlined in the consent form that they sign. If at any future date you wish to use the research data for any other purpose not previously specified at the point of the initial application, you will need to apply for further approvals, and get consent from participants for this.

- Consent to provide personal data must be specific and explicit. Blanket or implied consent will not be compliant with the GDPR. Participants must be clear what is being asked of them and have the right to exclude some types of activities where different types of data will be obtained from their overall consent.

- Researchers are responsible for reporting actual or suspected breaches of personal data security to the University's Data Protection Officer[1] at the *earliest possible opportunity* who will then assess whether the Information Commissioner's Office need to be notified. The University is legally required to report breaches within 72 hours.

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 participant data, opinions or beliefs, participants will need to be made fully aware in advance and provide specific consent.

Researchers should note that the terms 'pseudonymisation' and 'anonymisation' have specific means in the context of the GDPR that have been defined by the ICO[9].

For **staff research** the person responsible for all research data and records management is the lead researcher (as named on the form). For **student research** arrangements for the management of research data and records must be discussed and agreed between the student and the supervisor, and the student is expected to abide by the agreements reached; *the responsibility for managing confidential*

[7] http://www.hse.gov.uk/aboutus/meetings/hscarchive/2003/141003/c113h.pdf
[8] https://www.sussex.ac.uk/webteam/gateway/file.php?name=code-of-practice-for-research-june-2018.pdf&site=377
[9] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/

personal information provided by participants always rests with the supervisor as the University is legally responsible for this data.

Personal data should be managed with special care. It should:

- Be kept securely
- Remain retrievable
- Be accessible only to identified individuals according to clear access rules

Digital research data should be processed in accordance with University policies on Information Security[10]. This will include the use of encryption methods and only using institutionally approved data storage.[11] The principles of how data should be shared with the wider research community are set out in the *Research Data Management Policy*[12].

For **research overseas** the application should include information concerning any risks to the safety of research records arising from the local research setting. Normally, records should be transferred to the University as soon as possible – other arrangements will need to justified and thoroughly detailed. The onus is on researchers to fully understand local data legislation and how this may differ from the GDPR.

iv. Special Category Data

To legally process Special Category Data, in addition to the University's specified legal basis for processing (i.e. 'public task'), researchers are required to meet and be able to articulate an additional single set of conditions from the list below (Article 9,2 of the GDPR)[13]:

- Data has the explicit consent of the data subject
- Data is necessary for employment law or social security law purposes
- Data is necessary to protect vital interests
- Processing is by not-for-profit bodies or associations
- Personal data is manifestly made public
- Data is for the establishment, exercise or defence of legal claims
- Substantial public interest
- Medical purposes and the provision of health or social care
- Public health
- Archive, statistical and research purposes

Should Special Category Data need to be shared or transferred, robust encryption must be used. Such data should not be emailed unless security is assured and the researcher is confident that no breach of data integrity will result.

For further advice, researchers should contact the data governance team – dpo@sussex.ac.uk.

[10] https://www.sussex.ac.uk/infosec/policies

[11] Researchers should not use personal email accounts and such as Google mail or Drop-box but ensure that approved University cloud storage solutions are employed - http://www.sussex.ac.uk/its/services/networkandstorage/filestorage. See also the University's Cryptography Policy - https://www.sussex.ac.uk/infosec/documents/isp08-cryptography-policy.pdf

[12] https://www.sussex.ac.uk/webteam/gateway/file.php?name=rdm-policy-oct-2014.pdf&site=269

[13] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

v. Data and Records Management Responsibilities

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]in a useful form should be archived and made available for re-use by other researchers whenever possible. Funders are increasingly making data archiving a condition of their support.

Unanonymised personal data can be legitimately retained and reused for further research under the terms of the GDPR. However, its use must remain within the scope of the participant's original expectations and any published results must be anonymised. **If unanonymised data is to be used then participant consent must be secured at the outset.**

vi. What About Potential Obligation to Disclose Information?

[14] http://www.sussex.ac.uk/ogs/policies/information/recordsmanagementguidance
[15] The application for ethical approval will have covered the extent of the personal information taken for the study. The informed consent of research participants will include how the records will be stored and managed.
[16] https://www.ukdataservice.ac.uk/manage-data/legal-ethical/anonymisation

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 a researcher to disclose information to an appropriate authority might override concerns about confidentiality.

Researchers are expected to identify all reasonable likelihoods concerning potential disclosure within the Participant Information Sheet and ensure that the participant is aware of situations where confidentiality may be an issue.

Potential obligations to disclose include:

- public interest (where there is a real or serious risk that another individual, or the public at large, may be put in danger by the participant);
- statutory provisions (including the Children Acts 1989 and 2004, the Public Health (Control of Diseases) Act 1984, Proceeds of Crime Act 2002 and the Terrorism Act 2006); and
- disclosures (e.g. evidence of professional misconduct) which the researcher is obliged to report in accordance with their own professional obligations.
- Researchers have a professional obligation to inform the appropriate authorities if it comes to light during a study that a child is under serious threat of abuse.
- Balance is necessary with issues of confidentiality. It is vital to respect the interests of participants but it is unnecessary to place excessive restrictions on data. Anonymisation and proper consent to disclosure will help ensure that data is protected but that it can remain useful throughout the study and beyond.

vii. Data and Records Management with NHS based participants

In addition to requirements to work within data legislation, researchers who handle NHS patient records and data for research purposes are responsible for understanding and working to standards and procedures established by partner NHS trusts[17]. In the event that such policies are not available, the 'Confidentiality: NHS Code of Practice' (2003)[18], published by the Department of Health, serves as a reference point for legal requirements and professional best practice across the whole organisation[19].

Special Category Data taken by the NHS for the purposes of patient care and then shared for the purposes of University research should be managed with the utmost care and all efforts should be taken to avoid any such data being processed or stored in University systems or held in paper form. When data of this type is indispensable for research, the highest standards of security involving digital encryption and the use of locked filing cabinets behind locked doors (or equivalent) should be used following

[17] See also https://understandingpatientdata.org.uk/

[18] http://webarchive.nationalarchives.gov.uk/20161101131024/http://systems.digital.nhs.uk/infogov/codes/confcode.pdf

[19] See also the MRC Ethics Series document, 'Using information about people in health research' - https://mrc.ukri.org/documents/pdf/using-information-about-people-in-health-research-2017/ and the MRC's e-learning module 'Research Data and Confidentiality'- https://byglearning.com/mrcrsc-lms/course/index.php?categoryid=1

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 provide as much detail as possible in protocols and to participants about how such data will be taken, transferred, stored and finally deleted or archived whilst preventing possible data breaches or data loss.

viii. Data sharing agreements and institutional assurances of compliance

Researchers and supervisors of student research do not have the authority to sign data sharing agreements or enter into legally binding arrangements or reassurances for the management of data on behalf of the University. The Research Governance Officer in Research and Enterprise Services shall be approached in the first instance to advise on the most appropriate course of action.

[20] http://www.sussex.ac.uk/staff/research/governance/sponsorship

Ethical Considerations Relating to Gaining Consent

i. Informed Consent

Research participants must have the right to choose whether or not they will participate in research, and obtaining *INFORMED* consent is central to the ethical conduct of all research involving human participants. Fully informed consent in this context means consent freely given with proper understanding of the nature and consequences of what is proposed. The following process is recommended to ensure that this is in place:

- Each participant should be given an oral explanation.
- Each participant should then normally be given an **Information Sheet** explaining in simple, non-technical terms, what participating in the research will entail, any potential risks and hoped-for benefits.
- The participant should be given reasonable time to consider this information and to consult others as necessary.
- Except in the case of self-completion questionnaire based studies, the participant should usually be asked to sign a **consent form** (this should normally be witnessed in the case of vulnerable participants to ensure that the participant has understood the explanation and freely consents to enter the study).
- For research taking place in non-literate situations, or under other exceptional circumstances where obtaining written consent is either impossible or inappropriate, the researcher should clearly state the reasons why written consent is not being sought, and outline how consent (such as **verbal consent**) will be obtained and recorded in another way.

To ensure compliance with the GDPR, participants must be informed of what information will be held about them and who will have access to it (this relates to personal, identifiable information). Explicit and specific consent must be given when personal data is processed, including for questionnaire based studies. It is recommended that researchers use the following sentence with a tick box option on the Consent Form:

'I consent to the processing of my personal information and data for the purposes of this research study. I understand that such information will be treated as strictly confidential and handled in accordance with the General Data Protection Regulation (GDPR) 2016.'

Important special considerations relate to research projects involving **children**: please refer to the guidance for researchers produced by the National Children's Bureau *Guidelines for Research with Children and Young People* [21]

If it is proposed that research be conducted on persons who are not able to give fully informed consent on their own behalf justification for this must be clearly stated. Although consent cannot be given on behalf of another, it may sometimes be important to inform and/or enlist the support of those involved in the care of

[21] https://www.researchgate.net/publication/260060346_NCB_Guidelines_for_Research_With_Children_and_Young_People

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 **Mental Capacity Act 2005** which came into force on the 1st of October 2007. If you wish to carry out research involving individuals who lack capacity you must apply to an NHS REC after securing University Sponsorship[22]. https://www.hra.nhs.uk/.

You should note that research projects can be approved under the Mental Capacity Act *only* if the research cannot be carried out without the participation of individuals with the 'impairing condition' *and* the research is specifically connected to that impairing condition. Where a participant loses capacity during a research project, researchers may use the data which has been collected before the onset of incapacity, but must exclude that participant from that point until they regain capacity. Alternatively they should contact an NHS REC and submit a new application which, if approved, would then permit them to use this group of participants.

ii. Right of Withdrawal

Participants have the right to withdraw their participation at any time. This must be explained and respected throughout the research process. Researchers must not pressure any participants to re-engage with the research. It must also be made clear on all Information Sheets that the right to withdrawal extends beyond actual participation (to cover research data) and that researchers should make it clear at what point withdrawal of data is no longer possible (give a cut-off date). Please give an account of the circumstances in which participants might discontinue the study, and under what circumstances the study as a whole would be stopped. Please note that, while it acceptable for researchers to set a cut-off point for the withdrawal of data being used within the project, this cut-off point should not be at the convenience of the researcher but rather what is reasonable given the constraints of the project.

iii. Consideration of Relationship between Researcher and Potential Participant

Where the **relationship between recruiter and potential participant might be influential**, i.e. if prospective participants are colleagues or students of the researcher, this must be acknowledged. Please also provide an explanation of how you will deal with predictable problems resulting from the prior relationship (i.e. how will the researcher counteract a perceived pressure to participate on the part of the volunteer, how will the risk of potential confidentiality/anonymity breaches be minimised and what level of anonymity can realistically be guaranteed, what will happen if the researcher comes upon data suggesting professional misconduct, etc). If there are any **conflicts of interes**t in undertaking the research, this should be drawn attention to and you should indicate how these will be managed or mitigated

In **action research/research into your own workplace**, you must evaluate the extent to which your own role impinges on the research process. It is recognised that students often have dual roles, and may be studying and carrying out research whilst continuing an additional professional role. Students for whom this applies often choose to conduct their research project in their place of work. If this is relevant to your research, you may find it useful to read a King's College London guidance paper: *Research in the Workplace.* This guide includes some of the common conflicts

[22] http://www.sussex.ac.uk/staff/research/governance/sponsorship

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) - https://ico.org.uk/

MRC Regulatory Support Centre - https://mrc.ukri.org/research/facilities-and-resources-for-researchers/regulatory-support-centre/

EU GDPR Portal - https://www.eugdpr.org/

JISC - https://www.jisc.ac.uk/gdpr

Understanding Patient Data Project (supported by the Wellcome Trust) - https://understandingpatientdata.org.uk/

HRA e-learning - https://www.hra.nhs.uk/planning-and-improving-research/learning/e-learning/ - NHS e-learning is free of charge to researchers using ac.uk addresses. Includes the module 'Confidentiality and information governance considerations in research'

NHS England Information Governance - https://www.england.nhs.uk/ig/

NHS Digital - Data security and information governance - https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance

University Library - Research data management
http://www.sussex.ac.uk/library/researchdatamanagement/

UK Data Service - https://www.ukdataservice.ac.uk/manage-data/legal-ethical

University Privacy Notice -
http://www.sussex.ac.uk/ogs/policies/information/dpa/privacynotice

Data Protection Act (2018)
http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

University Information Security policies and procedures

Online University GDPR Training Module (University login required)
http://www.sussex.ac.uk/staffdevelopment/opportunities/staffdevelopmentcourses/onlinelearning

Bring Your Own Device Policy
https://www.sussex.ac.uk/infosec/documents/isp03-byod-policy.pdf

Information Security Policy
https://www.sussex.ac.uk/infosec/documents/isp01-information-security-policy.pdf

Information Handling Policy
https://www.sussex.ac.uk/infosec/documents/isp07-information-handling-policy.pdf

Cryptography Policy
https://www.sussex.ac.uk/infosec/documents/isp08-cryptography-policy.pdf

Institutional Access to information within University IT Accounts, Equipment and Networks Policy
https://www.sussex.ac.uk/infosec/documents/isp10-institutional-access-policy.pdf