Code of Practice for SOAS staff and students: Using Personal Data in Research

Owner	Research & KE Delivery
Last Updated	Nov-2020
Approved	Research & Enterprise Committee
Version	5.1

Table of Contents

1. Purpose of this Code

1.1.1 This code of practice is concerned with the gathering and use of information about identifiable living individuals ("personal data") as part of research undertaken by members of SOAS. Following it will help researchers to ensure that their projects:

i. Meet the legal requirements of the Data Protection Legislation.
ii. Adhere to ethical requirements for researchers at SOAS, as they relate to the processing of data about identifiable living individuals.
iii. Consider intellectual property issues relating to information supplied by research participants.

1.1.2 This code applies equally to SOAS staff and students conducting research at any level, where the research involves gathering or using personal data. It was approved by the School's Research and Enterprise Committee (Chairs action) on 17 November 2020. The most recent updates were made during August/October 2020.

2. Personal Data and Ethical Review

2.1.1 Research proposals require ethical review, however particular attention is given to research which involves using or collecting personal data (involves human research participants). The School's Procedures for Ethical Review include full guidance for different members of the SOAS community.

2.1.2 All researchers are now required to complete the School's mandatory Epigeum Research Integrity Online Programme.[1]

3. Data Protection Legislation

3.1.1 From 25 May 2018, all research involving personal data must adhere to UK and EU Data Protection Legislation. The rules governing the use of personal data by UK-based institutions are set out in the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018. These laws work in tandem and apply to both staff and students undertaking research which involves the processing of personal data.

3.1.2 Any research by SOAS staff or students which involves gathering or using personal data must meet the requirements of Data Protection Legislation and respect the rights which it confers on individuals, in accordance with the School's Data Protection Policy.

3.1.3 The GDPR is a Regulation which harmonises data protection law across the EU, whilst the DPA 2018 makes provisions around processing of personal data in specific areas, including research.

[1] For academic members of staff with externally funded research grants, this has been made mandatory. Similar applies for post graduate research students at Upgrade to PhD. Students on undergraduate or postgraduate taught programmes are strongly encouraged to register and complete the course *prior* to undertaking any primary research related to their dissertation or ISP. Should that proposed research be deemed sensitive, then the successful completion of the research integrity course would be required.

3.1.4 There are seven key principles that are set out in the GDPR [Article 5] and these must form the basis to approaching the processing of personal data. Moreover, the GDPR mandates organisations like SOAS (and the staff who work for them) as being responsible for demonstrating compliance with those principles.[2]

3.1.5 Prior to research being undertaken that utilises personal data, researchers are now required to appropriately identify the lawful basis upon which that data can be processed.

3.1.6 The lawful basis for processing personal data relating to research activity is that *processing is necessary for the performance of a task carried out in the official authority vested in the Controller, and/or in the substantial public interest*. Consequently, the standard of consent as described in Article 7 of the GDPR does not apply. However, researchers are expected to obtain informed consent which meets all the requirements of research ethics and funding bodies. Please see section 4 below on informed consent.

3.1.7 Processing of 'special category data'[3] or criminal convictions/offences,[4] can only be carried out if an additional condition in Article 9 of the GDPR is met. It is SOAS' view that this would come within Article 9 (2)(j): *processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes*.

3.1.8 Article 89(1) of the GDPR requires that efforts are made to design projects with privacy in mind, to ensure respect for the principle of data minimisation. Such efforts include the pseudonymisation or anonymisation of data, so that it can no longer be linked to an identifiable individual. See the section below on anonymisation.

3.1.9 Failure to comply with this legislation can have serious consequences. The legislation gives individuals the right to sue for damages which they suffer because of violations, and the right to request an investigation by the Information Commissioner (the body which regulates data protection in the UK).

3.1.10 If the Information Commissioner determines SOAS has breached the provisions of the Data Protection Legislation, they can take enforcement action, which may take the form of an administrative fine. The fine tariff has increased substantially in the GDPR. Lower tier fines for serious procedural breaches can be penalised with fines of up to €10 million; breaches of the principles, data subject rights and restricted transfers of data (i.e. overseas without safeguards) can be penalised with fines up to €20 million.

3.1.11 Research funders increasingly require projects to have adequate protocols in place to protect personal data, provide evidence of consent processes, and may refuse to give funding to institutions which have poor data protection practices.

3.1.12 As high-profile cases involving the loss of personal data indicate, inadequate data security can lead to negative publicity and serious reputational damage.

---

[2] Further details regarding each of the principles can be viewed at: GDPR Article 5

[3] GDPR Article 9 (1): Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation

[4] GDPR Article 10

3.1.13 Where students are engaged in research, the School and the student will be joint Data Controllers. The collaboration between the student and their supervisor in setting the parameters and methodology for the research project gives rise to a situation where both parties determine the purpose and means of personal data processing.

3.1.14 Further guidance in relation to the above can be accessed via the Information Commissioner's Office webpage. Additionally, should refer to the Information Compliance Manager for points of clarification.

4. Getting Informed Consent

4.1.1 Informed consent is one of the central principles of research ethics. The process ensures that human research participants:

i. enter research voluntarily and can withdraw if they wish at any point
ii. have complete information and fully understand the research process
iii. know what it means for them to take part
iv. give consent before they enter the research
v. understand any risks that may be involved with participation

4.1.2 In practice this means it is a researcher's duty to:

i. provide research participants with comprehensive information about their research
ii. communicate the information about the research project in a way that can be readily or easily understood e.g. in a language and vocabulary with which research participants are familiar
iii. tailor the information to the culture or society in which the research is being conducted
iv. show sensitivity to cultural differences that may affect the consent process.

4.1.3 Consideration also needs to be given to the extent to which research participants are capable of giving or providing informed consent:

i. Every effort should be made to secure the informed consent of children and other potentially vulnerable groups (e.g. refugees, internally displaced persons, adults with learning difficulties etc), although it is recognised that informed consent may also require the involvement of a parent, guardian or other person with a duty of care. Parental consent must normally be sought for children.[5] Children who are capable of forming their own views should have the right to express their views freely in all matters affecting them, commensurate with their age and maturity.
ii. "Freely given" or voluntary consent means that the individual should not be under duress or pressured to participate; there should be no adverse consequences for them from refusing to participate in the project and no coercion (actual or implied) to participate in the project.
iii. Although you may need to negotiate consent with a "gatekeeper" or an organisation e.g. to talk to employees, you will need to go through the consent process with individual research participants.

[5] Research involving potentially vulnerable research participants will require approval from the Research Ethics Panel (REP) and may require an Enhanced DBS check to be undertaken. SOAS researchers will also be required to successfully complete the *Safeguarding Essentials* course.

4.1.4 There are two important stages to the consent process:

i. Giving Information - so that the research participant can reflect on the information they are given and are not placed under pressure to respond to the research immediately.
ii. Obtaining Consent - the researcher should then reiterate the terms of the research clearly e.g. as separate points and the participant gives clear consent for each point before agreeing to take part in the project as a whole.

It is important that the research participant should be given a reasonable amount of time to consider whether to consent and to ask questions before being asked to give their consent.

4.1.5 All researchers must document that they have undertaken a full consent process:

i. Without a record of the research participant's consent, there is more likely to be uncertainty over whether a project is ethically sound and has complied with Data Protection Legislation.
ii. Consent should be documented for each of the different activities involving a research participants data in your research project.
iii. Documented consent must be collected by researchers in a form that is most appropriate for the research context.
iv. It is usually expected that consent from research participants should be captured in an appropriate format.
v. Researchers should keep all documentation relating to the consent process used (including information sheets, consent forms, audio recordings etc) as evidence of how consent was collected.
vi. Evidence of consent should be kept for as long as you are using or holding the research data.
vii. When collecting personal data during fieldwork, it is likely that obtaining informed consent will be an ongoing activity, and the process of obtaining consent may evolve from that originally envisaged at the outset of the research.
viii. If the research moves in an unanticipated direction, be aware that consent may need to be renegotiated with participants, in accordance with the need for consent to be given for a specific purpose. Make sure that the project's research methodology addresses any potential limitations in the methodology for obtaining informed consent.

4.1.6 Written consent should be undertaken:

i. when research participants can, read, understand and sign forms easily and are not put off by written information or their first contact with researchers has been through the provision of written information.
ii. documented on a signed consent form based on the SOAS template consent form included at the end of this document.
iii. copied so that the consent form is given to the research participant to keep.

4.1.7 Verbal Consent should be utilised:

i. when literacy may be a problem.
ii. where there are cultural or political concerns with signing documents.
iii. where either the research and/or the participant could be put at risk by the existence of a physical record.
iv. where time for consent is limited e.g. a chance interaction between researcher and participant (although you should not use non-written consent as a substitute for planning).
v. when it is more appropriate e.g. for interviewing elite participants.

vi. the same as the process for written consent e.g. research participants must be given the same information about the project, have a reasonable amount of time before being asked for consent, and indicate consent to each element including in consent forms.
vii. audio recorded e.g. if data is gathered through recordings, the start of the recording should include the researcher reading out the project information sheet and asking the participant the questions included on a consent form.
viii. For particular categories of research participant, obtaining written consent may be problematic as it could jeopardise their anonymity and may discourage participation altogether.

4.1.8 In very exceptional circumstances researchers may not be able to document evidence of consent from research participants. If this is the case researchers must:
i. Record why a consent form or audio recorded consent could not be used
ii. Keep a record that the consent process was followed e.g. who, where, when and how
iii. Check if any funder requirements or other duties for data sharing may become an issue

4.1.9 Considerations of informed consent also apply to audio-visual and photographic material:
i. Films, sound recordings and images can be personal data if they capture an individual with enough clarity to allow them to be identified.
ii. Consent for recording or photography may not always be necessary e.g. in the UK images of public spaces or public activities in which individuals are captured incidentally are not usually seen as raising privacy issues or requiring consent. For example, a photograph of a high street showing shoppers walking up and down, or news footage of a public demonstration. Researchers should, however, be prepared to demonstrate their study in no way alters the usual behaviour of the people under scrutiny and that their privacy is respected.
iii. There are many legal uncertainties in this area; the courts have held that in some cases, individuals have a right to privacy in images of their activities carried out in public. Typically, this occurs where the image focuses on an individual, intrudes into their private life, is used without their consent, and there is no overriding public interest justification.
iv. Researchers should also be wary of importing UK concepts of what is “private” and “non-private” into other cultural contexts. Activities performed by a group in its own group space may still be regarded as “hidden” or secret to the group, even if performed in the open.
v. Researchers must be transparent with research participants about when recording or photography is taking place, and how the information will be used. When in doubt, following the recommendations for obtaining informed consent outlined above.
vi. Covert or “hidden camera” recording or photography (in which individuals are not aware that the process is taking place) raises serious ethical and legal concerns and should only be undertaken after full ethical review of the proposed research according to SOAS’s ethical review procedures and in accordance with the provisions of the Regulatory and Investigatory Powers Act 2000.

4.2.0 Considerations relating to informed consent for conducting surveys include:
i. If surveys are entirely anonymous (i.e. the researcher has no way of knowing the identity of the respondent) and there is no way of linking individuals to the data, then Data Protection Legislation does not apply.[6] However, it would still be good ethical research

[6] Researchers need to be alert not only the nature of the questions that are asked, but also whether the survey captures other information that is personal data, e.g. registration by way of an email address, mobile phone

practice to provide respondents with information about the nature of the project and how their responses will be used e.g. through an information sheet which states that consent is implied through participating in the survey.

ii. Survey data is personal data if respondents are identifiable, e.g. from information which they provide on the form or through other information which is available to the researcher and therefore informed consent must be obtained.

iii. If researchers want to contact survey participants again, the participants should be informed, and you will need to obtain fresh consent. Researchers should therefore consider the likelihood that follow up surveys will be required in the project planning phase.

4.2.1 Informed consent issues for personal data that is already publicly available include:

i. Data taken from sources such as published newspapers or magazines, public websites, documents that are available for public inspection without restriction in a library or archive, there is generally no need to seek consent.

ii. In situations where it appears that the personal information was published without the consent or contrary to the wishes of an individual care should be taken and consent should be obtained from the individual before using the information.

4.2.2 Researchers can use personal data they have not collected directly from research participants themselves (e.g. information from a previous research project; data held in NGO records to which the researcher has been given access) without contacting them to inform them of the processing, providing the following conditions are met:

i. There may be occasions where contacting the individual to provide them with information about the processing of their data proves impossible or would involve a disproportionate effort and is likely to render impossible or seriously impair the research objectives (e.g. the participant's address, location or other means of contact may not be known or may change without the researcher's knowledge). In such cases SOAS will take appropriate measures to protect the individual's rights and freedoms and legitimate interests, including making the information about the research that will be undertaken publicly available on our website.

ii. The data must not be used to "*support measures or decisions with respect to particular individuals.*" In other words, the information must be used solely for research purposes, and not in ways which directly affect individuals.

iii. Use of the data must not cause or be likely to cause substantial damage or distress to the individual or, if sensitive personal data is used, any other person. This can be done by publishing and disseminating the information in anonymised form.

4.2.3 Processing of sensitive personal data from other sources is permitted in research under Article 9(2)(j) of the GDPR, and Schedule 1, Part 1, section 4 of the DPA (2018), provided that these conditions are met:

i. The data is not used in such a way that it will support measures or decisions with respect to individuals

ii. The data will not be used in such a way as to cause or be likely to cause damage or distress to the individual

iii. The processing is necessary for archiving/scientific/historical research purposes or statistical purposes.

number or the like. Moreover, the online tracking via cookies, IP addresses, analytics etc would have to be disabled.

4.2.4 It is still always best practice that if it is possible to contact the research participant to seek their consent (e.g. because recent addresses are available), the project should do so. Consent should then be captured in the same way as for projects which gather information directly from the individual. Individuals who refuse consent should be excluded from the project, and consent should not be inferred from the failure of an individual to respond to a communication.

4.2.5 Issues of informed consent for existing information used from data archives can include:

i. Datasets provided by external data services (like the Office for National Statistics or the UK Data Archive) will usually consist of fully anonymised data. As there is no way of identifying the individuals involved, such datasets can be used without thinking about informed consent.

ii. Non-anonymised datasets may also be available in some cases and typically under specific licences, terms or conditions or special access arrangements which are designed to protect the interests of research participants. There is no need for the customer to independently seek the consent of data subjects. However, when using datasets from external suppliers, any licensing agreements or restrictions imposed by the data supplier **must** be followed.

4.2.6 Considerations of informed consent when using Social Media in research:

i. The use of Social Media data in research is a quickly evolving landscape with a variety of ethical dilemmas and considerations of whether data is public or private and whether informed consent is required.

ii. Researchers will need to assess whether consent is sought from the individual, moderator or platform owner.

iii. If information is taken from forums, chat rooms, groups etc. then it is good ethical practice to inform members and seek consent from each individual member and keep evidence

iv. Researchers should wherever possible contact Twitter users directly if they will use their tweets in research. Researchers must remember it is easy to identify an individual from their Twitter ID when linked with other information.

v. There may be limitations of use of data placed on the social media platform. Researchers should also check general Terms and Conditions of Use.

vi. Researchers at the University of Aberdeen funded by the ESRC have written a paper addressing some of these challenges which includes case studies for different types of use of social media in research. If you are considering using Social Media in your research it is recommended you read this paper 'Social Media Research: A Guide to Ethics'. If you have any concerns about your plans to use Social Media in your research, please contact the School's Information Compliance Manager.

4.2.7 Research participants have the right to withdraw their consent at any time therefore:

i. researchers must provide research participants with the option to withdraw consent and provide clear information about how to do this.

ii. researchers must consider what the easiest way is for research participants to make contact and leave contact details which are practical e.g. postal address, phone number, email.

iii. researchers must reply promptly to all withdrawal requests.

iv. researchers should comply with all withdrawal requests, unless the withdrawal of the participant's consent would prevent or seriously impair the fulfilment of the research project's objectives. Researchers should note that refusing a withdrawal request must be a defensible decision, and that it can only be made if the researcher has taken steps to

safeguard personal data as described in Article 89(1) of the GDPR, including appropriate security measures and measures to reduce the risk of individuals being identified (by using methods such as pseudonymisation)

v. if you are unsure how to handle a withdrawal request or are going to refuse a withdrawal request you must contact the School's Information Compliance Manager for additional advice (see contacts list below).

vi. researchers must keep a record of any withdraw requests received and how they have been handled.

4.2.8 Informed and voluntary consent should be an ongoing process with the research participant:

i. Consent may need to be renegotiated with the research participant e.g. if the aims of the research or the methods of disseminating results change.

4.2.9 Useful examples of consent in specific research settings and other consent forms and are also available on the website of the UK Data Archive.

5. Collecting the 'Appropriate' level of Personal Data

5.1.1 Researchers should remember that Data Protection Legislation requires that personal data should be **adequate, relevant** and **not excessive** in relation to the purpose for which it was gathered. This is referred to as the principle of data minimisation.

5.1.2 Considerations on how much data is appropriate should relate to the goals and objectives of the research project.

5.1.3 Researchers must avoid any temptation to collect more data about individuals than is necessary for the project e.g. information which might possibly be of some use in the future, but for which no immediate use is envisaged.

6. Building Anonymisation into Research as Early as Possible

6.1.1 An important component of the GDPR is 'Privacy by Design', a concept that privacy and data protection should be considered from the outset of the research project. One way of achieving this is by anonymising personal data as early as possible. Doing so may seek to provide the appropriate mitigation for any ethical concerns that could be raised from research involving human participants.

i. Planning anonymisation before you start research will result in clearer informed consent for your research participants.

ii. Anonymising early on in research can help to ensure personal data is not released in contravention of the Data Protection Legislation.

iii. Once the information is anonymised, it ceases to be personal data, and can be disseminated and published without contravening Data Protection Legislation.[7]

6.1.2 Anonymisation techniques can include:

[7] GDPR Recital 26: The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

i. Removing variables which directly identify a research participant e.g. a name or address.
ii. Replacing identifiers with a code that cannot be linked to the identifier by a key.
iii. Reducing specificity of information e.g. referring to a region, rather than a town or village; using year of birth and not a date of birth.
iv. Restricting the upper and lower ranges of a dataset e.g. to remove outliers which could be easily identified.
v. Planning in advance with research participants what information should not be referred to in an interview e.g. company name.

6.1.3 Researchers must take care when:

i. anonymised data could potentially be combined with other available data to identify an individual e.g. even the first element of a postcode could identify an individual living in remote and sparsely populated postal district.
ii. original data is retained which still includes identifying information. As this is still personal data it will have to managed securely in according to Data Protection Legislation. It will remain personal data unless the research disposes of or anonymises the identifying information.
iii. individuals can be identified from other contextual information that may be included in research outputs etc. even if direct identifiers have been removed.

6.1.4 Anonymisation is a complex area. The following resources are useful sources of information on anonymisation:

UK Data Archive Anonymization Guidance

UK Anonymisation Network Anonymisation Decision Making Framework

ICO Anonymisation Code of Practice

6.1.5 Anonymisation should not be used interchangeably with the term pseudonymisation. The two terms are not the same thing.[8]

7. Working Securely with Personal Data

7.1.1 Good data security is an essential part of ethical research practice and is a requirement of Data Protection Legislation. Unauthorised access to personal data or accidental loss of data can have serious consequences for research participants and may damage the reputation of SOAS and the individual researcher.

7.1.2 The data security procedures which are appropriate for a project will depend on the sensitivity of the information. Not all personal data is equally sensitive.

i. Information about individuals which has already been published or is publicly available may need little or no protection. Similarly, information about individuals' public lives (e.g. their job title, office or rank, the identity of their employer) will generally be less sensitive than information about their private lives and may not require extensive protection.

[8] "Pseudonymising data means replacing the attributes in personal data – which make it possible to identify the data subject – with a pseudonym, and keeping those attributes separate, under technical or organisational measures." *Handbook on European data protection law*, 2018 edition, p. 131

ii. Conversely, strong security measures will be necessary for sensitive personal data, personal financial information, or information whose disclosure might cause individuals loss, harm or distress. As a rule of thumb, it should be assumed that harm could result from any unauthorised disclosure of information which relates to private life: e.g. home contact details, income, personal relationships or beliefs.

iii. The processing context is also a factor in determining appropriate technical and organisational security measures. For instance, if the project involves investigation of culturally or politically sensitive issues then any information which might identify a participant should be subject to stricter security measures.

7.1.3 Anonymisation can play an important role in ensuring data security.

i. As it is not personal data, an anonymised dataset can be used in a lower security categorisation than the version in which individuals are identifiable.

ii. A copy of the anonymised dataset could be kept on a researcher's laptop for analysis and writing up, with the data that identifies individuals kept solely at SOAS.

iii. As far as possible, non-anonymised personal data should *only* be stored on SOAS support systems, where it will be backed up automatically and protected by the School's security systems.

7.1.4 Most data security breaches occur when data is "on the move":

i. As many high-profile cases demonstrate, laptops and storage devices such as data keys/flash drives, CDs/DVDs and portable hard drives are particularly vulnerable to theft and accidental loss.

ii. Non-anonymised personal data should only be transported on portable devices where absolutely necessary.

iii. When portable devices are used to transport personal data, individual files containing personal data on research participants should be protected by password or other suitable encryption method if the information includes sensitive personal data, financial information about individuals, or information whose disclosure or loss could cause harm or distress to individuals.

iv. Passwords or encryption keys should be sent or stored separately from the data

v. If the postal service has to be used to transfer personal data, the data should be sent by recorded delivery and the storage media encrypted.

vi. Secure email or SOAS supported cloud storage is preferable to the post as a method of sharing personal data if required.

7.1.5 It is a researcher's duty to store personal data securely throughout the research projects lifecycle.

i. Access should be restricted to those individuals who need access to the data for the purpose of the research project: for example, by restricting access to and/or password protecting individual files (physical and digital).

ii. Personal data in paper format (e.g. consent forms signed by research participants) should be kept in a secure area or a locked filing cabinet when not in use. Where more than one person has access to the information, a booking system should be used to keep track of files.

iii. Data is vulnerable when it is being used at home, because of the increased risk of theft and unauthorised access. SOAS provides staff with secure remote access to SOAS systems or secure cloud service via MySOAS accounts (see the IT Department's guidance on Remote Access to files).

iv. To prevent accidental loss of data, researchers should regularly back up personal data onto SOAS provided systems, for example when on fieldwork. The same level of security should be applied to backup copies as to the original data.
v. Researchers should take care to delete local copies of any files including personal data (e.g. downloaded on laptops or home PCs) unless this comprises part of your backup strategy
vi. Research that involves use of the School's IT systems must conform to SOAS's IT policies and procedures, which establish the conditions of use for the School's systems.

7.1.6 Data protection also extends to when data is processed by one organisation on behalf of another.
i. This could arise when you have outsourced the gathering and analysis of survey data; have asked somebody to transcribe information which included personal data; have employed a translation service to translate data into a different language. These third parties, who process data on your behalf, are called Data Processors.
ii. It is the researcher's duty to ensure that you have entered into a contract which imposes obligations on the Data Processor to ensure they have security measures in place and will protect research participants' information. The terms of the contract must be in line with the provisions set out in Article 28 of the GDPR.
iii. The Research and KE delivery team can provide advice and examples of agreements and contracts used in these situations and the Information Compliance Manager can also be contacted.

7.1.7 Personal data gathered in research projects should be disposed of securely when it is no longer needed.
i. Before disposing of any data researchers must ensure they meet funder and SOAS policies for data retention.
ii. Data in paper format should be disposed of as confidential waste or shredded on-site if highly sensitive.
iii. Electronic data must be deleted and emptied from the recycle bin. For sensitive data you should seek to overwrite files using services recommended by the UK Data Archive
iv. Data held in SOAS email accounts must be deleted from inboxes, sent items and trash folders.
v. Advice from the IT Department can be requested on secure data disposal and secure and environmentally friendly methods of hardware disposal, if required.

7.1.8 Responsibility for data security should be established early on in research projects
i. Where a project team involves more than one individual, one team member should be assigned responsibility for data security e.g. including backup schedules and data transfer.
ii. The project team should agree and document the procedures which they will follow to keep data secure.

7.1.9 For further guidance on data security, contact the Information Compliance Manager or see the guidance on the IT Department's website and Research Data Management webpage. The Information Compliance Manager may refer you to the IT Department or Research Data Services for further assistance where necessary.

8. Retention and Disposal of Personal Data

8.1.1 Data Protection Legislation sets down the general principle that personal data should not be kept for any longer than is necessary for the purposes for which the data was gathered. However, Data Protection Legislation contains an exemption which allows personal data to be retained *indefinitely* for research purposes and allows for the fact that data may have value that persists for a considerable period of time after the completion of a project. However, data can only be kept provided both of the following conditions are met:

i. The data must not be used to "***support measures or decisions with respect to particular individuals***." In other words, the information must be used solely for research purposes, and not in ways which directly affect individuals.
ii. Use of the data must not cause or be likely to cause **substantial damage** or **substantial distress** to any individual who is the subject of the data [researchers can ensure this by: only publishing and sharing anonymised data; implementing strict data security etc.]
iii. As a general rule of thumb research data should be kept for a period of 10 years after completion of the project.

8.1.2 The exemption for research does not remove the need to comply with other principles of Data Protection Legislation:

i. Processing of data must be lawful, fair and transparent.
i. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
ii. Ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage
iii. If as a researcher you plan to use existing personal data in a new research project you will need to provide research participants with information about the new project and get their consent, unless they consented to the use of the data in specific future projects when the data was originally collected.
iv. The information supplied to research participants, consent forms and other records which document the obtaining of consent must be kept for at least as long as the data is kept.

8.1.3 Researchers with external funding should check funder requirements for the retention, archiving and sharing of research data (see below).

9. Research Participants' Rights to Access Personal Data held about them

9.1.1 One of the most fundamental rights granted to individuals by the Data Protection Legislation is the right to gain access to the information which organisations hold about them. However, under Data Protection Legislation the right of access does not apply to personal data processed for research purposes, where the right would prevent or seriously impair the objectives of the research. This exemption from the right of access is available on the basis that:

i. Technical and organisational measures are in place which enable the researcher to respect the principle of data minimisation, and in particular enable the researcher to employ pseudonymisation techniques to safeguard personal data.
ii. Where the purposes of the research can be fulfilled by anonymising data so that individuals can no longer be identified, the researcher should ensure that the data is anonymised.
iii. The processing is not likely to cause substantial damage or distress to the individual

iv. The processing is not carried out for the purposes of measures or decisions with respect to a particular individual.

10. Publishing and Sharing Personal Data

10.1.1 Researchers must ensure that any dissemination of personal data is in line with Data Protection Legislation:

i. Research participants should not be identified in published research results, PhD theses or in publicly available datasets, unless they have consented to being identified, or the information is already in the public domain.
ii. This applies equally to data obtained directly from the individual, and confidential personal data obtained from third parties.
iii. Even if you have consent for individuals that their identification is disclosed, it is a researcher's ethical duty to anonymise if disclosure would cause harm to the research participant.
iv. Providing research participants with a copy of the final research results or research publications, while not mandatory (or always practical), will support openness and transparency in research and should be seen as good practice. In any such arrangement, deadlines for comments should be set, and it should be agreed that editorial control remains with the researcher.

10.1.2 Many funders now require you to share your research data and researchers must ensure that this requirement is reflected in consent procedures (see template information sheet and consent forms below).

i. Research funders will often expect that anonymised research data is deposited in a recognised data archive e.g. UK Data Archive or Zenodo
ii. Researchers are expected to share data as openly as possible, but it may be necessary for access levels to be controlled because of the sensitivity of data. Funders expect researchers to address any barriers to research data sharing e.g. by anonymising datasets for deposit in an archive.
iii. Researchers who are required to deposit data in a data archive will also need to provide documentation relating to the research data: method of data collection; equipment used to analyse data; questionnaire and survey templates; blank consent forms.

10.1.3 For further advice about data sharing and archiving and funder policies please contact researchdata@soas.ac.uk

11. Ownership and Responsibilities for Research Data after leaving SOAS

11.1.1 The following considerations relate to SOAS staff:

i. Primary legal responsibility under Data Protection Legislation, for the personal data which staff gather and use as part of the formal records of a research project rests with SOAS, as the employer and the "data controller".

ii. Staff have no right to remove such data without SOAS's permission. Doing so could potentially compromise the rights of research participants, e.g. by causing data to be moved to an environment with inadequate security.
iii. Staff who wish to take non-anonymised research data with them at the end of their employment must ensure that they comply with Data Protection Legislation for the personal data they continue to hold.
iv. Staff must seek permission from their head of department, who will contact the Information Compliance Manager for advice. Staff who are granted permission will be required to sign a confidentiality agreement stating they agree to comply with Data Protection Legislation, the School's Research Ethics Policy and any undertakings made to research participants. A copy of the data **must** be saved to the SOAS network.

11.1.2 The following considerations relate to SOAS students:

i. Students are individually responsible under the Data Protection Act for personal data which they gather and use in their studies, although students are required in their research to abide by this code of practice and the School's Research Ethics Policy.
ii. Students may take personal data gathered by them in their research with them when they leave the School, unless the research was conducted as part of a SOAS research project in which the student participated, or the agreement with the funder or sponsor of the research specifies otherwise.
iii. However, students are reminded that they must continue to meet the requirements of the Data Protection Act and other legal and ethical requirements when storing and using the data.

12. Intellectual Property and Personal Data

12.1.1 Researchers should note that research participants have intellectual property rights in the information which they contribute to a research project. It is important that researchers deal with intellectual property issues early on in their research to avoid any issues arising.

12.1.2 Research participants are likely to own copyright in the words written by them on a questionnaire (but not the questionnaire itself) and what they said in an interview which was recorded in some way, and their delivery of their words.

12.1.3 While it is held outside the UK, information gathered overseas will be covered by any intellectual property laws which apply in the country of origin. Once the research data is imported into the UK, it will be protected under UK copyright law (with very few exceptions) in the same way as information created in the UK.

12.1.4 Research participants' intellectual property rights persist even if their identity is removed from their contribution: e.g. an individual will own copyright in their words recorded in an anonymised transcript of an interview.

12.1.5 Research participants do not own copyright in information produced by the researcher as a result of analysing the 'raw' research data: for example, statistics, abstracts or research conclusions.

12.1.6 The School's Research Ethics Policy requires that researchers should respect the intellectual property and other legal rights of research participants.

12.1.7 Intellectual property rights should be included as part of the consent process by ensuring that research participants are provided with full information about how their contributions will be used and consent to that use. The template consent forms in the Appendices includes clauses relating to copyright which are designed to achieve this.

12.1.8 For further advice on intellectual property issues, contact the Information Compliance Manager.

13. Where can I get further support and information?

Further information about Data Protection, Data Management and Security, Intellectual Property and Ethics issues is available at SOAS. Any student or staff undertaking research with human participants must seek appropriate information from the below sources and contacts:

SOAS Information Compliance Pages

SOAS Research Ethics Pages

SOAS IT Policies and Procedures

SOAS Research Data Management Pages

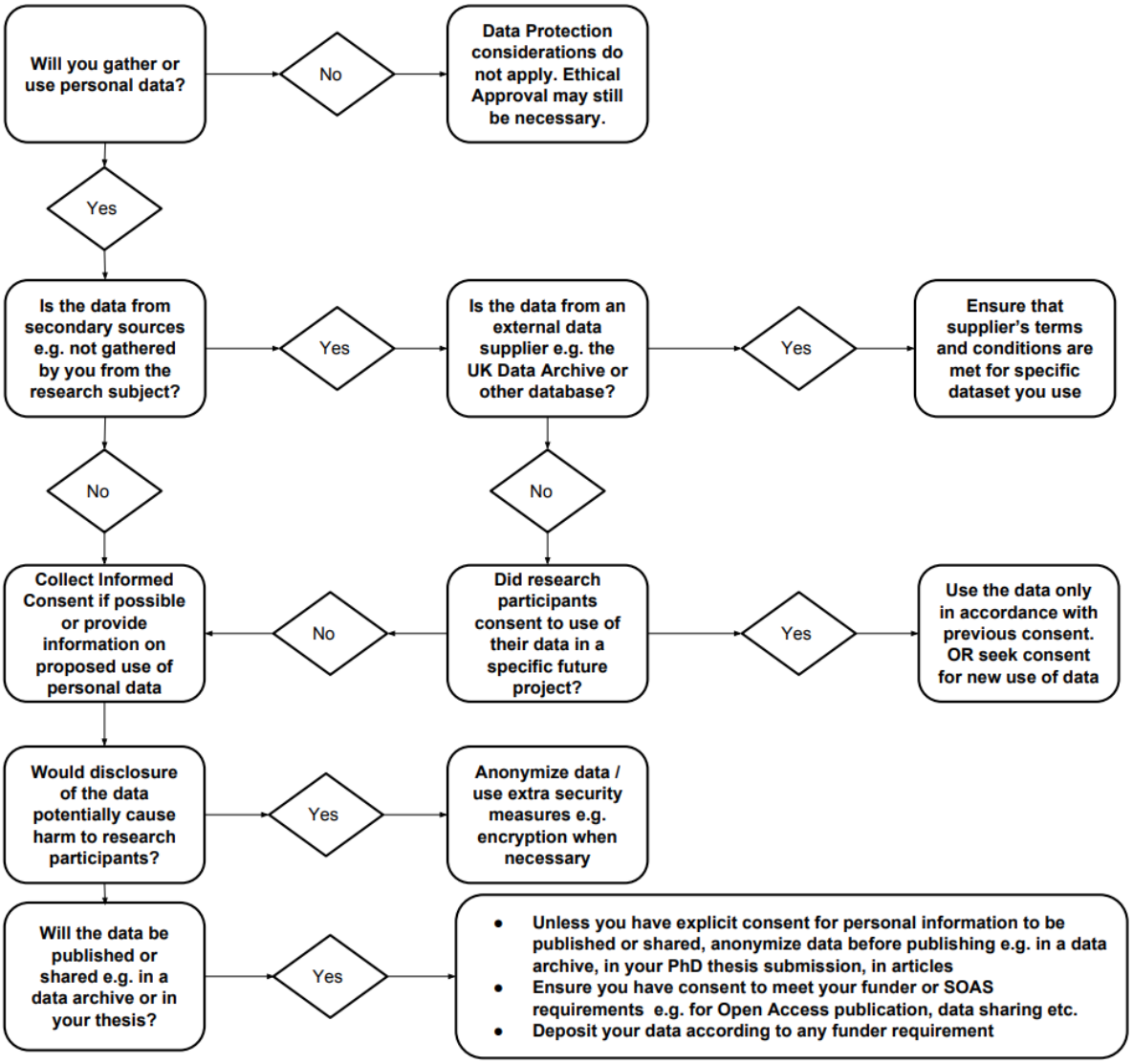
Legal Team

The following are key contacts for further inquiries:

- The Information Compliance Manager - dataprotection@soas.ac.uk or 02078984817
- Research Data Management Services - researchdata@soas.ac.uk or 0207898417
- IT Help Desk - helpdesk@soas.ac.uk
- Contracts - contractsteam@soas.ac.uk

Appendix A: Checklist for using Personal Data in Research

This checklist will help researchers to identify whether they have covered key issues relating to the use of personal data in their research project.



Appendix B: Research Participant Information Sheet Template

Information Sheet For [*Insert Title of Research Project*]

Introduction

The purpose of this form is to provide you with information, so you can decide whether to participate in this study. Any questions you may have will be answered by the researcher or by the other contact persons provided below. Once you are familiar with the information on this sheet and have asked any questions you may have, you can decide whether or not to participate. If you agree, you will be asked to fill in the consent form for this study or record your consent verbally.

Research title:	[Include both the official an alternative title if the official title of your thesis or project would be difficult for research participants to understand]
Name and contact details of researcher	[Give the name and work contact details of the person (usually the researcher) who is responsible for the project]
Name and contact details of Principal Investigator	[Give the name and work contact details of the principal investigator of the research project if applicable]
What type of research project is this?	[e.g. PhD Research, Funded Research Project, Non-Funded Research Project]
Who is funding this research project?	[Include the funders of the project, and any interest which they may have in the research or control over use of the research e.g. requirements for data sharing]
Who else is involved with the research project?	[Include any other organisations (e.g. other HE institutions) which are involved with SOAS in delivering the project, and what involvement they may have with access, analysis and holding of data]
What is the research project's purposes?	[Describe background, aims and duration of the project in as clear a language as possible and simple enough to be understood by research participants]
Why have I been chosen?	[Describe why you have chosen the research participant for your research project and data collection and who how many other participants will be involved]
Do I have to take part?	[Explain that taking part in the research project is entirely voluntary and that the participant can discontinue participation at any time]
What will happen to me if I take part?	[Describe the procedures involved with the research project e.g. how long the research will last and how long the participant's contribution will last. Describe the methods of data collection e.g. interviews; surveys; who will collect the data. Your research methods should be set out as simply as possible]
Will I be recorded and how will the recordings be used?	[Explain the recording method you will use e.g. video or audio, whether the recordings will only be used for analysis, whether recordings will be transcribed and how, who else will have access to the recordings]

Risks and Benefits of participation	[Explain any benefits for the participant in being involved in the research and also any risks, inconvenience or distress that could be caused by participation. State clearly if there are no intended benefits to the participants from taking part]
What if Something Goes Wrong?	[Inform participants how complaints will be handled should they arise or if something serious occurs during or following participation in the project]
Will I be recorded and how will the recordings be used?	[Explain the recording method you will use e.g. video or audio, whether the recordings will only be used for analysis, whether recordings will be transcribed and how]
Where will information I provide be transferred to?	[Indicate any specific countries to which the data may be transferred, including the UK if the data is gathered outside the UK.]
How will information I provide be kept secure?	[Describe in a general way any special security measures which will be put in place to protect research participants' data during the life of the project e.g., secure storage, backup procedures password protection]
Will I be kept anonymous in this research project?	[Data Protection legislation has the expectation of 'privacy by design'. If participants can be anonymised this should be done, and you should describe the steps which will be taken to remove identifying information from your data set and publications. If it is not possible to fully anonymise someone's identity you should state it here and on your Consent Form]
What will happen to the results of this research project?	[Describe how the data and the research results will be published, including whether research participants will be anonymized in the published information and where this published information will be available e.g. included in your PhD theses which will be made Open Access via the internet. Include plans or requirements to archive research data e.g. in data archives]

Data Protection Privacy Notice

The data controller for this project will be SOAS University of London. The SOAS Data Protection Officer provides oversight of SOAS activities involving the processing of personal data and can be contacted at dataprotection@soas.ac.uk

Your personal data will be processed for the purposes outlined in this Information Sheet. The legal basis that would be used to process your personal data under data protection legislation is the performance of a task in the public interest or in our official authority as a controller. However. for ethical reasons we need your consent to take part in this research project. You can provide your consent for the use of your personal data in this project by completing the consent form that has been provided for you or via audio recording of the information sheet and consent form content.

Your Rights

You have the right to request access under the General Data Protection Regulation (GDPR) to the information which SOAS holds about you. Further information about your rights under the Regulation and how SOAS handles personal data is available on the Data Protection pages of the SOAS website (http://www.soas.ac.uk/infocomp/dpa/index.html), and by contacting the Information Compliance

Manager at the following address: Information Compliance Manager, SOAS, Thornhaugh Street, Russell Square, London WC1H 0XG, United Kingdom (e-mail to: dataprotection@soas.ac.uk).

If you are concerned about how your personal data is being processed, please contact SOAS In the first instance at dataprotection@soas.ac.uk If you remain unsatisfied, you may wish to contact the Information Commissioner's Office (ICO). Contact details, and details of data subject rights, are available on the ICO website at: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/

Copyright Notice

The consent form asks you to waive copyright so that SOAS and the researcher can edit, quote, disseminate, publish (by whatever means) your contribution to this research project in the manner described to you by the researcher during the consent process.

Contact for Further Information

[*Give a point of contact for further information (both during and after fieldwork if they are different. This could be your name, address, email or telephone or that of another researcher on the project*]

Thank you for reading this information sheet and for considering taking part in this research study.

Appendix C: Research Participant Consent Form Template

Consent Form for [*Insert Title of Research Project*]

Please complete this form after you have read the Information Sheet and/or listened to an equivalent explanation about the research

Project Title: [*Insert title in same form used on your information sheet]*

Researcher Name: [*Insert name of researcher undertaking the research*]

Please tick the appropriate boxes	Yes	No
I have read and understood the project information sheet dated DD/MM/YYYY, or it has been read to me.		
I have been able to ask questions about the project		
I understand that potential risks of participating in this research include *[insert risks you have detailed on the information sheet] OR [delete if there are none*]		
I agree to take part in the project and understand that taking part involves [*insert a few words about how you will do data collection with the research participant, using the same terms as you did on the information sheet*]		
I agree that my interview is recorded [*using audio or video*]		
I understand that I can refuse to answer questions		
I understand that my taking part is voluntary; I can withdraw from the study at any time by notifying the researcher/s involved and I do not have to give any reasons for why I no longer want to take part		
I understand that my withdrawal or refusal to take part will not affect my relationship with [*insert name of organisation, school, university etc] OR [delete this entry if there is no organization involved with the research or research participant*]		
I understand that that personal information collected about me that can identify me, such as my name or where I live, will not be shared beyond the research team		
I understand information I provide will be stored securely by *[insert how you will protect research participants information*]		
I understand that the information I provided will be used for *[insert what you will use the participants contribution for and where e.g. PhD thesis. publications, reports, web pages, archiving and other research outputs*] and made available [*insert how items will be published e.g. on SOAS Research Online, online through publisher websites*] ***If you are a doctoral researcher or your research is externally funded please read notes below**		

I would like to be named in publications, reports, web pages, and other research outputs [*delete this if you intend to anonymise all research participants in your outputs*]		
I would NOT like to be named in publications, reports, web pages, and other research outputs [*delete this entry if you intend to anonymise all research participants in your outputs*]		
I understand that my information will be anonymised so that I cannot be identified in [*insert what you will use the participants contribution for and where e.g. publications, reports, web pages, and other research outputs OR delete this entry if you will give research participants a choice about identification*]		
I agree to waive copyright and other intellectual property rights in the material I contribute to the project		

Contact Information

Telephone No: [*include a UK mobile number and the local phone number you will use or set up*]

Email Address:

Postal Address:

Alternative contact: [*include your supervisor's name and contact details or other colleagues on your research project*]

Research Participant Declaration

Name of Participant [printed]	Signature	Date

I have accurately read out the information sheet to the potential participant and to the best of my ability, ensured that that participant understands what they are freely consenting.

Name of Researcher [printed]	Signature	Date

Please ensure a copy of this document is retained safely for future reference.

Appendix D: Notes on Adapting the Template Information Sheet and Consent Form

General

i. All SOAS Researchers can use and adapt the template Information Sheet in Appendix B and the Consent Form in Appendix C
ii. Any proposed changes to the privacy and copyright notice will need to be pre-approved prior to usage.
iii. Information provided in your Information Sheet should match the statements you provide in the Consent Form
iv. The text coloured red in the Information Sheet and Consent Form templates are notes about what the researcher should include. Replace the text with specifics about your own research
v. It is very important that these forms are adapted appropriately for your research participants e.g.
    - by using clear language (non-technical language simple enough to be understood by uneducated persons and full enough so they can understand the purpose of your research)
    - by translating them into the language spoken by research participants if they are not confident with English or you are not confident they can fully understand the form in English
    - by changing the look and feel if a formal layout is not appropriate e.g. if you are researching with children
vi. PhD researchers must explicitly mention that their thesis will be available made available in SOAS Library and online via SOAS Research Online
e.g. 'I understand that the information I have provided may be included in a PhD Thesis which will be available in SOAS Library and online via SOAS Research Online'
vii. Researchers with external funding must explicitly mention plans and requirements for data archiving
    - e.g. I give permission for the [specify the data e.g. anonymised transcripts of interviews, audio recordings, survey] that I provide to be deposited in [insert name of data archive e.g. UK Data Archive or Zenodo] which will be made available [insert access levels e.g. publicly available, registered users, request access]
viii. For researchers who have requirements or intend to deposit their data in a data archive you should consider access levels, so you can include this on your consent form and information sheet
ix. You must explain realistically the possible risks to the research participant including emotional/psychological ones and explain any steps you will be using to ameliorate these
x. If you are researching within an organisation e.g. NGO, company, university etc. make it clear that they must not discriminate against anybody who doesn't want to participate in your study
xi. Copies of the completed consent forms must be retained for audit purposes.

Appendix E: Key definitions

Term	Definition
Data Protection Legislation	General Data Protection Regulation (EU 2016/679) and the UK Data Protection Act (2018) and any successor legislation binding in the jurisdiction of the university.
Personal Data	Information relating to an identified or identifiable living individual/natural person (data subject): one who can be identified directly/indirectly by reference to an identifier (e.g. a name) or, one of certain specific characteristics relating to the individual.
Special Category Data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
Processing	In relation to information, means an operation or set of operations which is performed on information, or on sets of information, such as: collection, recording, organisation, structuring or storage, etc.
Lawful basis for the processing of Personal Data	*Processing is necessary for the performance of a task carried out in the public interest.*
Lawful basis for the processing of Special Category Data	*Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.*
Anonymisation	Anonymous information, namely: information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.
Pseudonymisation	Processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
Data minimisation	(Personal data shall be): adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Appendix F: Useful Links

SOAS Data Protection Policy
https://www.soas.ac.uk/infocomp/dpa/policy/

Research Ethics at SOAS
https://www.soas.ac.uk/research/ethics/

Research Data Protection Impact Assessment (DPIA)
https://www.soas.ac.uk/research/ethics/file138283.pdf

Concordat to Support Research Integrity (Oct-2019)
https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Documents/2019/the-concordat-to-support-research-integrity.pdf

EC Ethics in Social Sciences & Humanities
https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020_ethics-soc-science-humanities_en.pdf

SOAS Mobile Device Information Security Guide
https://www.soas.ac.uk/itsupport/information-security-guide/

SOAS Research Data Management
https://www.soas.ac.uk/scholarly-communication/research-data-management/

SOAS Open Access Policy
https://www.soas.ac.uk/scholarly-communication/open-access/file123991.pdf

SOAS OneDrive Guide
https://ble.soas.ac.uk/pluginfile.php/4443328/mod_resource/content/0/OneDrive%20Guide%20at%20SOAS.pdf

UK Data Archive
https://www.data-archive.ac.uk/

Epigeum Research Integrity Course (version 2.0)
https://www.soas.ac.uk/research/ethics/research-integrity-online-programme/