Data Protection and research

This is a guidance note for researchers at the School working with personal data. The Data Protection Act (DPA) covers how personal data should be processed. Personal data is any information that identifies a living individual, including opinions about that individual and/or any intentions a data controller has towards that individual. Personal data collected and used for research is covered by the DPA. However, the School's Research Ethics policy also applies, and covers personal data relating to the deceased.

The important sections of the DPA for research are:

- eight data protection principles that govern how personal data should be processed
- two schedules
  - Schedule 2 contains the conditions by which most personal data can be processed
  - Schedule 3 contains the conditions by which sensitive personal data can be processed
- Clauses relating to making requests
  - for information held
  - to have information corrected

Researchers have to consider how they manage personal data from the point they start collecting it, through storage to disposal. What you tell research subjects about your project when it starts could determine how and where you could deposit the data at the end of it.

JISCLegal is also producing guidance, which will be linked to when it is available.

The Data Protection principles and research

1 Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless — (a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

Personal data must be collected and used in accordance with the DPA. This principle means that individuals should know who is collecting the research, where it will be kept and what will be done with it. If you are collecting the data, you should have some form of privacy notice associated with the collection so that people are aware of what you will be doing with their data. For research studies, this is usually done by way of an information sheet and/or informed consent form. Researchers should refer to the LSE Research Ethics Policy and Procedures and guidance on Informed consent. In addition, the Information Commissioner's Office provides useful guidance on how best to write a privacy notice, available here: privacy notice code of practice.

Schedules 2 and 3 set out the conditions by which personal data can be processed. Sections 1 and 6(1) of Schedule 2 are most likely to apply to research data. Section 1 applies when the individual concerned has given their consent to the use of their data in the research. Section 6(1) applies where a staff member or research student at the School has a legitimate interest in using the data and this use won't harm the individual concerned. Where ever possible, consent should be gained from the individual you are collecting information from. However, if you are unable to do so because you have not had direct contact, section 6(1) should apply.

There may be some research projects where gaining informed consent is not possible or very difficult e.g. anthropological research where observation is the mode of research and gaining consent would interfere with the observation. Section 6(1) could apply as long as the research subjects' data is anonymised and will cause them no harm to process. The Association of Social Anthropologists ethical guidelines contain a useful list of issues to consider when negotiating consent for research as well as what to avoid in Section 1 (4) and (5). The British Sociological Association's statement of ethical practice also offers guidance in this area.

Information that has been made publicly available by the individuals concerned can be used without consent, though it would still be worth anonymising personal data where possible.

Care needs to be taken to ensure that consent is meaningful and freely given. Employees who have been told to participate in research by their organisation cannot be said to have freely consented to participating in research. Some children and vulnerable adults may be able to consent, but parents and guardians may need to give consent on their behalf.

Schedule 3 covers the sensitive personal data, which are covered in a separate section below.

2 Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

If you are reusing a research data set someone else has collected for further research, the exemption under Section 33 applies. This section allows for any personal data to be reused in research providing that it is not processed to support measures or decisions relating to particular individuals or processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject.

Where Section 33 applies, principle 2 does not stop processing of the data for other research. It also allows for personal data to be kept indefinitely despite principle 5 (see below) and subject access (see below) does not have to be given provided that the results of the research or any resulting statistics are not made available in a form which identifies data subjects.

If you are being required by a research funder or intend to deposit the data in an open repository in anonymised or any other form so it can be used by other researchers, tell research subjects you are doing so when collecting the data.

3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Only collect the personal data you really need for your project. Consider what is really necessary for your project before you start as to get informed consent (see above) you will need to explain to research subjects why you need their personal data.

4 Personal data shall be accurate and, where necessary, kept up to date.

Personal data collected for research is likely to be a snapshot of a moment in time. As such, it is unlikely to need updating. Long term collections will be keeping to this principle anyway for the purposes of future research.

5 Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

As stated above, research data is exempt from principle 5. This doesn't mean that you shouldn't consider how long to keep data. You should consider destruction of the original dataset once an anonymised or other form is in an open digital repository, for instance. Contact the Data Librarian for more guidance on retention.

6 Personal data shall be processed in accordance with the rights of data subjects under this Act.

As stated above, research data is exempt from subject access. However, it may be better to release data if it will be helpful for a research subject to know what we hold and it is best to ask them to check transcripts, etc so that they have the chance to correct any incorrect data.

7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Personal data should be kept securely so that no unauthorised access can occur.

Paper/hard media should be:

- kept in lockable cabinets/cupboards when not in use
- kept in lockable offices if possible
- not left lying on desks if you will be away from your desk for a considerable period of time

Electronic data should:

- Not be displayed where third parties can inadvertently see it
- Not be forwarded to third parties accidently – always check email addresses
- Be encrypted or password protected in transit
- Be kept on secure network drives or password protected/encrypted removable media.
- Once the School provides an extra secured area on the network, research data that has either of the following characteristics should be stored in the extra secured area:
    - been specifically required by a research funder to have extra security OR
    - contains sensitive personal data
    - needs the extra security in the opinion of the Information Security Manager and/or Information Rights team

8 Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Get explicit consent for sending data outside the European Economic Area (the EU plus Norway, Iceland and Liechtenstein) if you are at all likely to be processing it outside those countries. You should be fairly safe in countries like Canada, Switzerland and some other countries listed here, which have comparable laws to the DPA. Use password protection or encryption where possible in transit, but bear in mind that some countries will require you to provide the encryption keys if you take personal data into them.

Processing sensitive personal data

The DPA defines certain data as being sensitive personal data, requiring more stringent processing. The sensitive personal data are:

- Race or ethnic origin
- Political opinions
- Religious or similar beliefs
- Trade union membership
- Physical or mental health
- Sexual life
- Criminal or alleged criminal offences
- Participation or alleged participation in court proceedings

As well as meeting one of the Schedule 2 conditions, one of the Schedule 3 conditions must be met for the processing of this data. In this case, it is almost impossible not to get explicit informed consent to process as the only conditions that are possible for research are:

1 The data subject has given his explicit consent to the processing of the personal data.
5 The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

Explicit consent means you must be able to prove that the research subject knew what was being collected, how it would be used and how the data would be disposed of at the time it was collected. This means you will need a signature or mark on a form or bottom of a letter explaining the research or a tick box on an electronic form will need to be ticked.

Requests for information – Subject Access requests and corrections

Research subjects have two major rights under the DPA. The first is to request any information held on them and the second is to have erroneous information corrected or deleted. The School has never received either type of request from a research subject, but both remain a possibility.

Subject access requests are handled by the Information Rights team. A research subject that indicates to you that they want a copy of the data held on them should be directed to the email address glpd.info.rights@lse.ac.uk. We will process the request, which will involve filling out a form and providing the £10 fee and proof of ID. We have 40 days from receipt of the fee to provide any information held. Researchers will need to send the Information Rights team a copy of any information held as soon as possible, but no later than 39 days after the fee is received.

Requests for corrections and deletions have to be dealt with within 21 days. However, this means we must respond within 21 days. If a researcher has evidence that the information they hold is correct, the research data does not necessarily need to change. However, a note should be added to the effect that the research subject has challenged the accuracy of the data. While a research subject can ask for their data to be removed from a dataset, it will be very difficult to do so once the research has been published. There are no test cases in law for this situation. It could be a case of noting in any further research products that the dataset is slightly different if the data does need to be removed.

Anonymisation and Pseudonymisation of research data

Anonymisation should mean that a dataset has been cleared of any potentially identifying data before being published and/or released to third parties. However, true anonymisation is difficult to achieve if a dataset is to be useful for reuse. An ability to remove identifying data satisfactorily can lead to a pseudonymised data set, which has the obvious identifying data removed but leaves enough for a third party to identify the individual research subjects. As such, it is worth letting research subjects know if their data will be included in a published dataset and what you plan on including so as to minimise their identification.

The Information Commissioner's Office produced a code of practice for Anonymisation, which also includes methods for anonymising data.

Summary of Data Protection issues for research

You need to provide research subjects the following:

- The name of the project, its purpose and objectives.
- The identities of the organisations or individuals who have funded the research, and any interests they may have in the research.
- Why the information is being collected, and why it is necessary for the project.
- The name and contact details of the person who will be responsible for the data gathered in the project (usually, the researcher).
- Who will have access to the data, including any organisations or individuals outside the School who may be given access.
- Any special security measures which will be taken to protect the data.
- The countries to which the data may be transferred, including the fact that the data will be transferred to the UK (if the data is gathered outside the UK), and whether the data may be transferred outside the EEA.
- How the data will be published or made available, including whether research subjects will be identifiable in the published data, or whether the data will be published in anonymised form.
- Steps which will be taken to archive the data, e.g. by depositing a dataset in a data archive (e.g. one specified by the research funder or with the School), and whether the archived data will be anonymised or non-anonymised.

- How the data may be used in future research projects.
- How the research subject can withdraw their consent to participate in the project if they subsequently decide to do so.

Contacts

Rachael Maguire; email r.e.maguire@lse.ac.uk
OR glpd.info.rights@lse.ac.uk