Data Protection and Research

Guidance Note

1. Introduction

Personal Data used for research purposes by University staff must be dealt with in accordance with the Data Protection Act 1998 and its 8 Data Protection Principles. This is subject to the limited exemptions set out in Section 33 of the Act (see 4 below). The following guidance note will define personal data and outline the considerations and responsibilities of those conducting research involving personal data in the context of the Data Protection Principles.

2. Personal Data

The Act defines personal data as any information that relates to an identifiable living individual (the data subject) who can be identified from that data or from other information in the possession of, or likely to come into the possession of, the data controller.

The Act makes separate provision for personal information classed as sensitive personal data. Personal data will be regarded as sensitive where it relates to:

- Ethnic or racial origin
- Political opinions
- Religious beliefs
- Trade Union membership
- Physical or mental health
- Sex life
- Criminal offences or alleged criminal offences

This type of data is subject to further constraints on processing, requiring that certain additional conditions are met (outlined in 5.1.2 below).

3. Anonymisation of Personal Data

If personal data is suitably anonymised then it is outwith the scope of the Data Protection Act. However, the level of anonymisation must be such that it is impossible to identify any living individual from the information concerned or in combination with any other information that the University holds or is likely to hold – something which is difficult to achieve. For example, if you have removed identifying personal details from a list of respondents, but have given each a code from which their identity could be established, then this would not count as anonymised data and would be subject to the Act. If, on the other hand, identifiable personal details have been removed from the list and no ‘key’ exists that would allow their subsequent identification (and it is not possible to identify them from any other information held by the University or likely to be held by the University e.g. mailing list) then this would count as being completely anonymised and outwith the scope of the Act. It should be noted, however, that true anonymisation is difficult to achieve and it should not be automatically assumed that taking steps to anonymise data will mean that the provisions of the Act do not apply.

Data Classification: Public
4. Section 33 Exemption: Research Purposes

The Act gives certain exemptions from its normal requirements for “research purposes” (including statistical or historical purposes), which apply where the processing of the Personal Data is a) not used to support measures or decisions targeted at particular individuals, and b) does not cause substantial damage or distress to any individual. Provided these conditions are met, it is permissible to:

- Process the personal data for purposes other than that for which it was originally obtained (exempt from the second data protection principle). e.g. Data collected by the University for administrative purposes, such as enrolment forms, can be used for research purposes even though this was not originally intended.
- Hold data indefinitely (exempt from the fifth principle).
- Disregard the data subject’s right of access to their personal data, provided the data is processed for research purposes and the results do not identify data subjects.

5. Data Protection Principles

5.1 Principle 1: *Personal data shall be processed fairly and lawfully*

*Lawfully*

5.1.1 Certain conditions as set out in Schedule 2 of the act must be met before personal data can be processed lawfully. Those most likely to apply to research involving personal data are:

- Consent has been obtained from the research participant (data subject) for the processing of their personal data.
- The processing is necessary to pursue the legitimate interests of the University or third parties and is not unfair to the individual.

5.1.2 For sensitive personal data, as defined in 2. above, one of the normal Schedule 2 conditions of processing and one of the additional schedule 3 conditions must be met before processing can be carried out. Those most likely to apply to research involving sensitive personal data are:

- Explicit consent has been provided by the research participant for their personal data to be processed. Explicit consent should be in writing and involve a positive response from the participant i.e. it should be an 'opt in' rather than an 'opt out'. It is recommended that the researcher obtain a signed and dated consent from the individual which contains details of the project and how their data will be used.
- The research being conducted is medical research carried out by a health professional or someone who owes a similar duty of confidentiality.
- Analysis of racial/ethnic origins is being undertaken for equal opportunities monitoring purposes.

In addition to these conditions, the Data Protection (Processing of Sensitive Personal Data) Order 2000 expressly permits processing of sensitive personal data for research purposes which are 'in the substantial public interest' where the sensitive personal data are not used to support measures or decisions targeted at particular individuals without their explicit consent, and no substantial damage or distress is caused, or is likely to be caused. e.g. it may be permissible to obtain files of patients suffering a particular condition where the public interest in the research in terms of benefits to life and health is very great. However, caution should be exercised in relying on this condition as the test of “substantial public interest” is very high.
5.1.3 Under the “fair processing” requirements of the act, researchers also need to provide the following information to research participants – known as a “fair processing notice”:

- The identity of the researcher and their relationship with the University/department
- The purpose the data will be used for
- The identity of other people who may have access to the data.

This fair processing notice should be provided to participants at the time information is initially collected about them.

In some cases, the researcher may be using personal data obtained from a third party, rather than directly from the data subject. In such cases a fair processing notice should still be provided, unless it can be proved that providing such would involve disproportionate effort on the part of the researcher.

In deciding whether the disproportionate effort argument applies, researchers should evaluate the time, cost and ease of providing the subject with the notice against the benefit to the subject of receiving the notice (or prejudice in not receiving it). Factors to consider in this assessment would include the size of the sample, whether up-to-date contact details are available and if not, how easy or practical it would be to obtain them, the purpose of the research and its likely effect on the individuals concerned.

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

Provided the conditions of the s.33 exemption for research purposes (detailed in 4 above) are met, research data is exempt from this principle.

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

Researchers should only collect and process personal details which are necessary to conduct their research. For example, if personal identifiers such as names and addresses are not required in order to carry out the research, the respondent should not be asked for such information.

5.4 **Principle 4: Personal data shall be accurate and, where necessary, kept up to date.**

Efforts should be made to ensure that personal data gathered for research purposes is accurate. In most research situations it will not be necessary to keep the personal information updated as the research will be based on information representing a situation at a particular moment in time.

5.5 **Principle 5: Personal data processed for any purpose or purposes shall not be kept for longer than is necessary.**

Provided the conditions of the s.33 exemption for research purposes (detailed in 4 above) are met, research data is exempt from this principle.
5.6 Principle 6: **Personal data shall be processed in accordance with the rights of data subjects under this Act.**

The Act confers a number of rights on individuals in respect of personal data held about them. These include:

- **Right of access to personal data** – The right to be informed by the data controller (the University) whether the controller holds personal data on them, the purpose of the processing and to be given a copy of the information constituting the data.

Provided the conditions of the s.33 exemption for research purposes (detailed in 4 above) are met, research data is exempt from this principle. However, the remaining rights detailed below still apply:

- **Right to prevent processing likely to cause damage or distress** - The right to object to processing of personal data about them which the data controller must take account of. The individual must show that there are grounds for the objection in that the processing is unwarranted as causing, or being likely to cause, substantial damage or distress.

- **Right to prevent processing for purposes of direct marketing**

- **Rights in relation to automated decision making** – The right not to have significant decisions that affect them made solely by an automated decision making process.

- **Compensation for failure to comply with certain requirements** – The right to take action for compensation if they suffer damage or distress by any contravention of the act by the controller.

- **Rectification, blocking, erasure and destruction** - The right to take action to rectify, block, erase or destroy inaccurate data.

- **Assessment** - The right to request the Information Commissioner to make an assessment as to whether any provision of the Act has been contravened.

5.7 Principle 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.**

Researchers must employ measures appropriate to the sensitivity of the data held to ensure that personal data is kept securely. They should ensure that:

- Personal data held on computer is protected through appropriate access restriction and password protection controls. Digitised personal data should only be stored on shared network drives and not offline or on local drives.

- Personal data held manually is stored in locked cabinets and offices to prevent accidental or deliberate access by third parties.

- Personal data held off site (e.g. at home or travelling) receives the same level of security protection as it would in the office.

- Personal data is disposed of appropriately once research has been completed. For paper files this will mean disposal in confidential waste sacks for low level personal data, or cross shredding for sensitive personal data. For information stored on magnetic storage media (including computer hard discs) degaussing will be necessary to permanently erase the data. Physical destruction of the storage disc will be required for information stored on optical media.
5.8 Principle 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.*

This principle will need to be taken into account where research involves international collaboration and, in the course of that collaboration, personal data will be transferred to a country outside the EEA. In most cases explicit consent to the data transfer will be required from participants.

For further advice or assistance on this matter please contact the Data Protection Unit:

[Data.protection@stir.ac.uk](mailto:Data.protection@stir.ac.uk)

Updated January 2015