DATA PROTECTION IN RESEARCH

Document control	
Applicable to:	All employees and research students
Date first approved	February 2006
Date first amended	May 2015
Date last amended	**May 2015**
Approved by	1. Research Ethics and Governance Committee 2. Academic Board
Approval date	1. 13 May 2015 2. 25 June 2015
Review date	May 2018
Document owner	Research & Enterprise Development Centre

1. INTRODUCTION

1.1 Research is a crucial function of the University. Within disciplines such as education, social sciences and health, research often entails the processing of personal data, including sensitive personal data. There may also be instances when the University is involved in international research that may involve transfer of personal data overseas.

1.2 This document draws attention to the provisions of the Data Protection Act 1998 ('the 1998 Act') relating to research activities, and outlines actions required to achieve compliance with the Act.

1.3 The 1998 Act lays down principles of good information handling designed to ensure personal data is used in a way that is fair to individuals and protects their rights. The 1998 Act applies to personal data, that is data from which a living individual can be identified. It does not apply to generic information about companies, aggregated statistical data, or information about deceased individuals.

1.4 It is expected that all research and researchers will comply with all legal requirements and with University policies, procedures and guidelines, and in particular the University Data Protection Policy[1].

1.5 It is important to note the 1998 Act does not seek to protect data *per se* but to provide individuals with an element of control over the use of their personal data.

2. PRACTICAL IMPLICATIONS OF THE DATA PROTECTION ACT 1998 FOR RESEARCH

2.1 The practical implications of the 1998 Act are that:

2.1.1 Researchers must ensure that processing of personal or sensitive data takes place only when there is a clear purpose for doing so

2.1.2 Individuals must be informed of the uses to which their data will be put (i.e. the collection, use and distribution of their personal data)

2.1.3 Confidentiality must be maintained in the use of personal data and the identity of individuals must be protected

2.1.4 It must be remembered that individuals have the right to prevent the use of their data if they feel that it would be disadvantageous to them

2.1.5 All data must be stored both properly and securely.

3. DEFINITIONS

3.1 **Personal data** is defined as that which relates to living individual who:

- Can be identified from that data
- Can be identified from that data and any other information which is in the possession of, or likely to come into the possession of, the data controller.

[1] Data Protection Policy (http://www.canterbury.ac.uk/university-solicitors-office/policies-and-procedures/data-protection.aspx)

3.2 **Data** is defined as any information which is:

- Processed automatically or recorded with the intention to process automatically
- Recorded as, or with the intention that it be, part of a manual 'relevant filing system' (i.e. a structured system identifying individuals)
- Contained in a health, educational or social services record.

3.3 A **health record**, for the purposes of the 1998 Act is one relating to the physical or mental health of an individual which has been made by, or on behalf of a health professional in connection with the care of that individual.

3.4 **Sensitive data** includes information about racial or ethnic origin, physical or mental heath or condition, and sexual life. Data subjects are any person from whom data/information is obtained. This means that, with the exception of anonymised or aggregated information, the majority of data collected from human subjects during the course of a research project - whether held electronically or on paper – will fall within the scope of the 1998 Act. Processing of data is widely defined and covers all manner of use including obtaining, recording, holding, altering, retrieving, destroying or disclosing data.

3.5 A **data controller** is responsible for the manner in which any personal data is processed. The data controller has the benefit of processing the data and decides what personal data should be processed and why. The University is the data controller. Individual members of staff or students who process data on behalf of the University are data users.

4. GENERAL PRINCIPLES OF DATA PROTECTION

4.1 All processing of data to which the Act applies must comply with the Data Protection Principles set out in Table 1.

4.2 The first principle is particularly important as it shows that processing must be fair and lawful in the context of both common law and other UK legislation. This will, in general, be complied with if:

- Confidentiality is upheld
- The data subject was not misled or deceived into giving the data
- The data subject is given basic information about who will process the data and for what purpose
- At least one of the conditions in both Schedules 2 and 3 are satisfied (Tables 2 and 3).

5. RESEARCH AND THE DATA PROTECTION ACT 1998

5.1 Researchers should be aware the processing of any information relating to an identifiable living individual constitutes 'personal data processing' and subject to the provisions of the 1998 Act, including the eight data protection principles set out in Table 1.

5.2 There are certain exemptions in the 1998 Act relating to the processing of data for research. These are defined by **Section 33,** and relate to **principles 2 and 5, and to Section 7**. These exemptions apply only where the data are *not* processed to support measures or decisions with respect to particular individuals. In addition, these exemptions apply only in cases where the processing of data for research will *not* cause

substantial damage and distress to any data subject. The definition of research includes historical and statistical analysis.

5.3 There are *no* blanket exemptions from the data protection principles set out in Table 1. It is important that those undertaking research, both staff or students, are aware that most of the Data Protection principles still apply. They need to be aware of where and when they apply. In addition, the criteria for these exemptions differ where *sensitive* personal data is processed.

5.4 Many purposes of data processing for research are not necessarily determined at the time data is obtained. For example, researchers might later use information collected by others. **Principle 2** requires personal data may only be processed for one or more specified and lawful purposes, which would exclude such processing of personal data for research where it was not specified at point of collection.

5.5 Research data is exempt from **principle 2**. Personal data obtained for other purposes, e.g. mark data collected to be used by Boards of Examiners, may be processed for research even if that purpose was not made explicit to data subjects. This means that use of such data for research, although obtained for other purposes, will not be incompatible with the purposes for which it was obtained (the second principle) though the researcher is obliged to give the subject general information about intended uses (as above).

5.6 Research data is exempt from **principle 5**. Thus, data processed for research may be retained indefinitely, and will not be considered "out of date" however long it may be held. Data may legitimately be further processed beyond its original purpose as long as the other conditions are met. For example, it is easy to visualise a situation where data collected in the course of a survey might later be seen to have other applications. This is permitted as long as:

- The identity of individuals is protected
- The data is not used to make decisions in respect of individuals
- No substantial damage or distress is likely to be caused to individuals.

6. SENSITIVE PERSONAL DATA

6.1 The conditions outlined in Schedules 2 and 3 apply to the processing of all personal and sensitive data (Tables 2 and 3).

6.2 The 1998 Act classifies certain types of personal data as sensitive. The following types of information fall into the category of sensitive personal data:

(a) ethnic or racial origin;

(b) political opinions;

(c) religious beliefs;

(d) trade union membership;

(e) physical or mental health;

(f) sexual orientation and behaviour;

(g) criminal offences or alleged criminal offences.

6.3 Inappropriate use of information of this kind is potentially prejudicial to the data subject; the 1998 Act requires extra precautions be taken when processing sensitive personal data.

6.4 The processing of *sensitive* personal data for research purposes may only be carried out if one of the conditions is satisfied (1998 Act Schedule 3, as set out in Table 3):

(a) the explicit consent (ideally in writing) of the data subject has been obtained.

(b) medical research is being carried out by a health professional or someone who owes a similar duty of confidentiality

(c) it is an analysis of racial/ethnic origins, carried out for the purpose of equal opportunities monitoring.

(d) the Data Protection (Processing of Sensitive Personal Data) Order 2000 allows for sensitive data processing which: 'is in the substantial public interest and is necessary for research purposes and does not support measures with respect to the particular data subject except with their specific consent nor cause or be likely to cause substantial damage and distress'.

7. FAIR PROCESSING OF DATA

7.1 Despite the exemption from **principle 2**, research data subjects should still be informed of any new purposes of data processing and the identity of the data controller and any disclosures that may be made. If this involves disproportionate effort then data controllers may avoid this obligation, noting in their records the reasons for believing that disproportionate effort would be required.

7.2 The data subject should still be informed of any new purposes of data processing and the identity of the data controller and any disclosures that may be made (**principle 1**). Such notification may be avoided if:

a) The data has been obtained directly from the data subject but the purpose of processing the data for research was not known at the time and it is subsequently deemed 'not practicable' to provide the relevant information (**Schedule 2 Pt II 2(1)b**).

b) The data has been obtained from a third party; and provision of such information would involve disproportionate effort; and no prior demand for information has been made by the data subject; and the data controller records the reasons for believing that 'disproportionate effort' applies. The Information Commissioner has advised that assessing disproportionate effort should include factors such as cost, time and ease of provision of information weighed against benefit to the individual. Where data is obtained from elsewhere, particularly if the data is not recent, then it may be impossible, or at least disproportionately difficult, to inform the data subjects.

7.3 Data subjects must be told who will process their data and the purpose for which it will be processed. They must also be given any other information that is necessary to ensure that processing is fair and lawful. In this context, it is important to know that individuals are entitled to prevent processing (and, therefore, to participate in research) if they believe that is will cause them or another person unwarranted or substantial harm or distress.

7.4 It is important also to note that any subject who suffers damage due to an unauthorised disclosure is entitled to compensation though the data controller will have a defence if it can be demonstrated that reasonable care was taken to comply with the 1998 Act.

8. SUBJECT ACCESS REQUEST

8.1 The 1998 Act gives individuals (data subjects) a number of rights including the right to access personal data organisations hold about them. Under section 7 of the Act, data subjects have a right of access to any personal data held by the University as data controller. This right of access extends to all information held on an individual, and includes personnel files, student record files, databases, interview notes and e-mails referring to the individual.

8.2 The data controller has to communicate to the data subject the information held in an intelligible form within forty days, and can charge a maximum of £10 for doing so (see Section 6 for more detail).

8.3 If an individual makes a request to view their information, it is known as a "Subject Access Request".

8.4 The Act stipulates that the data subject must:

- ⇨ make the request in writing (which includes transmission by electronic means)
- ⇨ provide enough information to prove who they are (to eliminate risk of unauthorised disclosure)
- ⇨ supply appropriate information to help the University to locate the information they require.

8.5 Upon receipt of a request, the University must provide:

- ⇨ information on whether or not the personal data are processed
- ⇨ a description of the data, purposes and recipients
- ⇨ a copy of the data
- ⇨ an explanation of any codes contained within the data.

8.6 Research data is exempt from **section 7** of the 1998 Act. Data processed for research are not open to subject access requests so long as the results of any research (in articles, research reports, dissertations etc) do not identify data subjects. This means such data are exempt from the subject access rights provided the results are not made available in a form from which individuals can be identified.

9. SECURITY OF DATA

9.1 The requirements for appropriate security of data laid down in **principle 7** must be respected including appropriate levels of security for sensitive data and security of data processed by researchers outside the institution. To increase the security of data processing, it is advisable to anonymise data to as great an extent as possible.

10. INTERNATIONAL RESEARCH

10.1 International research collaborations involving transfer of personal data may not be transferred to countries outside the EEA (**principle 8**) unless that country has adequate data protection regulations, or the explicit consent of the data subject has been obtained, or there is an appropriate contract with the recipient of the data, specifying appropriate data protection requirements that must be upheld. Thus, researchers must be exceptionally careful when contemplating the transfer of research data overseas. In most

cases, the safe option will be to ensure that data subjects give explicit consent for overseas transfer during data collection[2].

11. RESEARCH INTERNAL TO THE UNIVERSITY

11.1 Such data processing occurs in not only academic research, but also where administrative, academic or service departments carry out statistical analysis of personal data to study trends in performance, use of services, and the student experience.

12. FURTHER GUIDANCE

12.1 The advice in this document is complemented by our Research Ethics and Governance Advisory Note No.2 *Research data storage and retention* (January 2013)

(http://www.canterbury.ac.uk/centres/red/ethics-governance/REG_ADV_NOTE_2rev.pdf)

12.2 A JISC Legal paper *Data Protection and Research Data: Questions and Answers*, written by Andrew Charlesworth a well respected authority in the field, provides valuable guidance in relation to specific questions that might arise when individuals are undertaking research.

(http://www.jisclegal.ac.uk/ManageContent/ViewDetail/ID/3648/Data-Protection-and-Research-Data-Questions-and-Answers.aspx)

TABLE 1 SCHEDULE 1: DATA PROTECTION ACT (1998)

THE DATA PROTECTION PRINCIPLES

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.

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.

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

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

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

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

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.

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.

[2] For discussion relating to international schemes, see Data Protection Guidance on International Schemes, available from the Data Protection Officer.

TABLE 2 SCHEDULE 2: DATA PROTECTION ACT (1998)

CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE: PROCESSING OF ANY PERSONAL DATA

1. The data subject has given his consent to the processing.

2. The processing is necessary –

a) For the performance of a contract to which the data subject is a party, or

b) For the taking of steps at the request of the data subject with a view to entering into a contract.

3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

4. The processing is necessary in order to protect the vital interests of the data subject.

5. The processing is necessary –

a) For the administration of justice,

b) For the exercise of any functions conferred on any person by or under any enactment,

c) For the exercise of any functions of the Crown, a Minister of the Crown or a government department, or

d) For the exercise of any other functions of a public nature exercised in the public interest by any person.

6. **1.** The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

2. The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

TABLE 3 SCHEDULE 3: DATA PROTECTION ACT (1998)
CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE:
PROCESSING OF SENSITIVE PERSONAL DATA

1. The data subject has given his explicit consent to the processing of the personal data.

2. **1.** The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

2. The Secretary of State may by order-
a. Exclude the application of sub-paragraph 1) in such cases as may be specified, or
b. Provide that, in such cases as may be specified, the condition in sub-paragraph 1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

3. The processing is necessary-
a. In order to protect the vital interests of the data subject or another person, in a case where -
(i) Consent cannot be given by or on behalf of the data subject, or
(ii) The data controller cannot reasonably be expected to obtain the consent of the data subject, or
b. In order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

4. The processing-
a. Is carried out in the course of its legitimate activities by any body or association which -
(i) Is not established or conducted for profit, and
(ii) Exists for political, philosophical, religious or trade-union purposes,
b. Is carried out with appropriate safeguards for the rights and freedoms of data subjects,
c. Relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and
d. Does not involve disclosure of the personal data to a third party without the consent of the data subject.

5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

6. The processing-
a. Is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
b. Is necessary for the purpose of obtaining legal advice, or
c. Is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

7. **1.** The processing is necessary-
a. For the administration of justice,
b. For the exercise of any functions conferred on any person by or under an enactment, or
c. For the exercise of any functions of the Crown, a Minister of the Crown or a government department.

2. The Secretary of State may by order-
a. Exclude the application of sub-paragraph 1) in such cases as may be specified, or
b. Provide that, in such cases as may be specified, the condition in sub-paragraph 1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

8. **1.** The processing is necessary for medical purposes and is undertaken by-
a. A health professional, or
b. A person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

2. In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

9. **1.** The processing-
a. Is of sensitive personal data consisting of information as to racial or ethnic origin,
b Is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and
c. Is carried out with appropriate safeguards for the rights and freedoms of data subjects.

2. The Secretary of State may by order specify circumstances in which processing falling within sub-paragraph 1)a) and b) is, or is not, to be taken for the purposes of sub-paragraph 1)c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph.