PRINCIPLES OF ANONYMITY, CONFIDENTIALITY AND DATA PROTECTION

The Legal Framework:
1. The collection, storage, use, disclosure and destruction of research data by researchers must comply with the Data Protection Act 1998 and the Common Law Duty of Confidence. All personal information collected should be considered confidential information and be dealt with in such a manner, in order not to compromise the personal dignity of the participant or to infringe upon their right to privacy.

In summary:
If you are collecting, storing, using, disclosing or destroying identifiable personal information about living individuals, then you should ensure that you comply with the requirements of the Data Protection Act 1998 (DPA) and the Common Law Duty of Confidence (see paras 2 to 31).

If you are collecting, storing, using, disclosing or destroying identifiable personal information about deceased individuals, then you should ensure that you comply with the requirements of the Common Law Duty of Confidence (see paras 23 to 31).

If you are collecting, storing, using, disclosing or destroying anonymised personal information, whether relating to the living or the deceased, then your research activity falls outside the scope of these guidelines (see paras 32 to 41).

The use of identifiable personal information in research should be reduced so far as possible. You should think carefully about where it may be possible to use less identifiable data (e.g. Rather than collecting full date of birth, would it be sufficient to collect only ‘month and year’? Is it necessary to collect, or retain, full post-code?). All processing of personal information should be defensible as both relevant and accurate (see para 4).

If it is necessary to use identifiable personal information, then you should usually only use identifiable personal information with the consent of the data subject. It is possible to use such data without consent but consent is to be preferred unless it can be shown to be inappropriate for some reason (see paras 6 to 12).

When gathering identifiable personal information you should aim at all times to ensure that the processing is defensible as both ‘fair and lawful’. This requires you to be as transparent as possible about the uses to which data will be put and any risks involved (see paras 13 to 18).

You should ensure that personal information is kept secure at all times. The level of security should be proportionate to the risks but all personal information should be kept securely (see para 4, footnote 2).

You should not keep personal information for longer than necessary, but it is recognised that (so long as relevant conditions are satisfied) research may require the retention of data for long periods and this may be justified (see paras 19 to 20).

\[1\] see paragraph 3.
Personal data processed for research purposes may be exempt from a subject-access request (see paras 19 to 21).

You should avoid disclosing identifiable information, including information that may be identifiable to others, wherever possible. If it is necessary to disclose personally identifiable information, or information that may be potentially identifiable, then this should usually only be done with the consent of the individual/s involved (see paras 6 to 12 and 23 to 31).

The Data Protection Act 1998

2. The Data Protection Act 1998 (DPA) implements European Directive 95/46/EC into English Law. One of the purposes of the European Directive is to ensure a common standard for data processing across Europe so that the transfer of personal data can take place between European countries in an environment protective of fundamental rights and freedoms, in particular privacy.

3. The DPA applies to 'personal data' and that means:

Data which relate to a living individual who can be identified:

(a) from those data, or
(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

4. The DPA establishes eight principles of data protection. If research involves the acquisition, use or destruction or personal data, then a researcher must ensure that those personal data are:

- processed 'fairly and lawfully';
- obtained only for one or more specified and lawful purposes, and not further processed in any manner incompatible with that purpose or those purposes;
- adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
- accurate and, where necessary, kept up to date;
- not kept for longer than is necessary for that purpose or those purposes;
- processed in accordance with the rights of data subjects provided for under the DPA;
- protected by appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss, destruction, or damage;
- not 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.

5. In order to demonstrate that data are processed 'fairly and lawfully' (i.e. in order to satisfy the requirements of the first data protection principle) a number of minimum conditions must be satisfied:

6. If a data controller is processing 'personal data', then they must ensure that at least one of the conditions set out in Schedule 2 of the DPA is satisfied.
7. The first condition listed in Schedule 2 is that the 'data subject has given his consent to the processing.' If consent is practicable, then it is to be preferred to any alternative condition listed within Schedule 2.2 If there are valid reasons for not seeking consent, then the sixth condition listed in Schedule 2 states that processing may take place where '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.'

8. It is the view of the University Research Ethics Committee (UREC) that a researcher seeking to use personal data for ethically approved research may rely upon paragraph 6(1) if consent is not appropriate. Circumstances where consent may not be appropriate include those where obtaining consent is not possible, not practicable, or would substantially undermine the science of a research project e.g. the project involves principled deception. These circumstances are discussed fully in Research Ethics Policy Note No.2, 'Principles of Consent', and require particular caution and vigilance on the part of researchers: www.sheffield.ac.uk/ris/other/gov-ethics/ethicspolicy/policy-notes/consent

9. It is possible that any personal information used for research purposes will constitute ‘sensitive personal data’. The DPA defines ‘sensitive personal data’ as including the:

- racial or ethnic origin of the data subject;
- his or her political opinions;
- his or her religious beliefs or other beliefs of a similar nature;
- whether he or she is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992);
- his or her physical or mental health or condition;
- his or her sexual life;
- the commission or alleged commission by him or her of any offence, or
- any proceedings for any offence committed or alleged to have been committed by him or her, the disposal of such proceedings, or the sentence of any court in such proceedings.

10. If research involves sensitive personal data, then a data controller must be able to show that (as well as satisfying one of the conditions set out in Schedule 2 of the DPA) they are able to also satisfy one of the conditions set out in Schedule 3.

11. The first condition specified in Schedule 3 is that ‘the data subject has given his explicit consent to the processing of the personal data’. For most research involving sensitive personal data, this is likely to be the only appropriate condition. If ‘explicit consent’ is not practicable, then it is possible that research involving sensitive personal data may be able to

---

2 The processing of personal information, particularly sensitive personal information (see definition below), will engage an individual’s Article 8 right to a private and family life as recognised by the European Convention of Human Rights 1950. The Human Rights Act 1998 puts English Courts under a responsibility to interpret domestic law where possible to give effect to the Convention Rights, including the Article 8 right to a private life. For this reason, they may require any failure to obtain consent for the processing of personal data to be justified as necessary and proportionate in the circumstances. More pragmatically, under English Law, obtaining consent for the processing of personal information may avoid a breach of the common law duty of confidence. For both of these reasons, there are sound legal reasons for seeking consent where it is practicable to do so.
rely upon one of the other conditions set out in Schedule 3, particularly if the research is medical research.

12. Paragraph 8 of Schedule 3 makes it a relevant condition of processing ‘sensitive personal data’ that,

(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.

13. In order to demonstrate that data are processed ‘fairly and lawfully’ (in accordance with the first data protection principle), a researcher must, however, do more than simply demonstrate that at least one condition of Schedule 2 is satisfied (and, if relevant, one condition of Schedule 3). An additional minimum condition of ‘fair and lawful’ processing is the notification to a data subject of the purposes of processing.

14. Data will not be considered to be processed ‘fairly and lawfully’ unless ‘so far as practicable’ a data subject is provided with, or has made readily available to him or her,

(a) the identity of the data controller (or any nominated representative),
(b) the purpose or purposes for which the data are intended to be processed (e.g. whether video material might be used for teaching purposes), and
(c) any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair.

Such information would normally be made available as part of seeking an informed consent. It is important to note, however, that the DPA makes the provision of this information a responsibility even if one of the conditions (other than consent) is being relied upon to satisfy Schedule 2 (or Schedule 3).

UREC recommend that relevant ‘further information’ to be provided as a matter of routine, where practicable, would include information about:

• any potential risks that the confidentiality or anonymity of personal information cannot be guaranteed (see additional guidance at the end of this Specialist Guidance Paper);
• which individuals and organisations, if any, will be permitted access to personal information, and under what circumstances such access will be permitted.

15. If a data controller receives personal data direct from the data subject, then, in so far as it is practicable to do so, they should make the information referred to in Section 14, above, available to the data subject at the time that the data is received. More information, with examples, can be found under the sub-heading What about ‘privacy notices’? on the ICO website: www.ico.gov.uk/for_organisations/data_protection/the_guide/principle_1.aspx
16. If a data controller receives personal data from a third party, then they should make this information available to the data subject either when they receive the data from that third party, or, if they themselves intend to provide further access to a fourth party, at the time such access is provided.

17. If a data controller has received the personal data from a third party (whether or not they intend to disclose to a fourth), then they are excused the responsibility to provide this information to a data subject if doing so would involve a disproportionate effort.

18. It is not entirely clear what distinction is to be drawn between ‘practicable’ (in para 15) and ‘disproportionate effort’ (para 17) above. They are both terms used within the legislation and there is no clear indication what is to be implied by the choice of different words. What is clear, however, is that any failure to provide the information to a data subject would have to be defended; on the grounds of either impracticability or disproportionate effort.

Data Protection Act 1998 – Research Exemption

19. Section 33 of the Data Protection Act 1998 provides a research exemption:

(2) For the purposes of the second data protection principle, the further processing of personal data only for research purposes in compliance with the relevant conditions is not to be regarded as incompatible with the purposes for which they were obtained.

(3) Personal data which are processed only for research purposes in compliance with the relevant conditions may, notwithstanding the fifth data protection principle, be kept indefinitely.

(4) Personal data which are processed only for research purposes are exempt from section 7 if:

(a) they are processed in compliance with the relevant conditions, and

(b) the results of the research or any resulting statistics are not made available in a form which identifies data subjects or any of them.

20. The effect of this exemption is three-fold if research data are processed in accordance with the relevant conditions. First, it allows data collected for one purpose (‘X’) to be used for another research purpose (‘Y’), even when that research purpose has not been notified to a data subject, without infringing the second data protection principle. Second, it allows data processed only for research purposes to be kept indefinitely, notwithstanding the fifth data protection principle requirement that data only be kept for as long as necessary to perform the specified purpose(s). Third, it restricts a data subject’s rights - specifically their right to access personal data held by a data controller - and so modifies the meaning of the sixth data protection principle.

21. It needs to be noted, however, that Section 33 does not affect the applicability, scope, or nature, of the other data protection principles and they continue to apply. For example, the requirements of ‘fair and lawful’ processing set out in the first data protection principle. If a data subject is not informed of an intention to process their (sensitive) personal data for a specific research purpose because it is not practicable to do so (or it would involve a disproportionate effort), then this would not constitute a breach of the first data protection principle.

---

3 “the relevant conditions”, in relation to any processing of personal data, means the conditions - (a) that the data are not processed to support measures or decisions with respect to particular individuals, and (b) that the data are not processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject.
disproportionate effort), then the research exemption ensures that processing for research purposes in such circumstances does not represent a breach of the second data protection principle. It does not modify the responsibility to notify in the first place, so far as it is practicable to do so.

22. The DPA applies to the processing of identifiable information relating to living persons. Satisfaction of the requirements of the DPA does not, however, automatically discharge any responsibility that an individual owes under the Common Law Duty of Confidence. If the requirements of the DPA are satisfied, then it is still necessary to be able to demonstrate that a particular use of confidential information takes place either (1) with consent or (2) is in the ‘public interest’.

Common Law Duty of Confidence

23. The Common Law Duty of Confidence applies to research involving confidential personal information. Under the law of confidence, it is recognised that individuals have a reasonable expectation of privacy in relation to confidential information: any use of confidential information that exceeds that which an ordinary person could reasonably be said to expect will constitute a breach of confidence.4

24. Information will be considered confidential if an individual could be understood to have an objective reasonable expectation that the information will, in the circumstances, be kept private.5

25. The easiest way to affect an individual’s reasonable expectations is by explaining clearly what will happen with their personal information. Minimally, it should be made clear who will have access to their data, for what purpose(s), and for how long. Special considerations apply, and further specific advice should be sought, if considering seeking consent from children (0-18),6 from vulnerable persons with capacity to consent,7 and vulnerable persons

---

4 In Murray v Express Newspapers plc and another [2008] EWCA Civ 446, [2009] Ch. 481, 502-3, para 36, Sir Anthony Clarke MR said, ‘As we see it, the question whether there is a reasonable expectation of privacy is a broad one, which takes account of all the circumstances of the case. They include the attributes of the claimant, the nature of the activity in which the claimant was engaged, the place at which it was happening, the nature and purpose of the intrusion, the absence of consent and whether it was known or could be inferred, the effect on the claimant and the circumstances in which and the purposes for which the information came into the hands of the [party alleged to owe the duty of confidence].’

5 In Coco v A N Clark (Engineers) Ltd [1969] RPC 41, Megarry J said, at p 48: ‘It seems to me that if the circumstances are such that any reasonable man standing in the shoes of the recipient of the information would have realised that upon reasonable grounds the information was being given to him in confidence, then this should suffice to impose upon him the equitable obligation of confidence.’

6 See, for example, General Medical Council advice on involving children or young people in research: ‘0-18 years: guidance for all doctors’ (paragraphs 36-40) (www.gmc-uk.org/guidance/ethical_guidance/children_guidance_36_40_research.asp) and ‘Consent to Research’ (paragraphs 14-18) (www.gmc-uk.org/guidance/ethical_guidance/6469.asp). Note that the Department of Health ‘Guidance for Access to Health Records Requests’ (February 2010) states that ‘The law regards young people aged 16 or 17 to be adults in respect of their rights to confidentiality. Children under the age of 16 who have the capacity and understanding to take decisions about their own treatment are also entitled to decide whether personal information may be passed on and generally to have their confidence
26. If the intention is to use confidential information for a research purpose, then that should be clearly explained to an individual and their consent, either express or implied, sought for such use.

27. It should also be made clear to an individual that there is an ongoing entitlement to withdraw consent to the processing of data for specific purposes.

28. Researchers must make clear to participants any intention to provide third party access to confidential information - including after the project’s conclusion. Without an express indication to the contrary, access must be restricted to the lead researcher and researchers directly involved in the research. Where practicable, personal information that could identify participants should remain anonymous at all times, even to the researchers themselves (although such cases are likely to be unusual).

29. A researcher may not disclose the identity of a person, or disclose any information that could identify that person, without having obtained, in advance, that person’s consent to do so, preferably in writing. If the research process is such that it is unavoidable that participants should in some circumstances be explicitly identified to others - perhaps e.g. other participants - then the researchers should explain why this is the case, and how best possible confidentiality will be maintained.

30. Researchers should be aware of the risks to anonymity, confidentiality and privacy posed by technologies of personal information storage and processing which directly identify a person: audio and video recordings, electronic and paper-based files, and e-mail records. Measures to prevent accidental breaches of confidentiality should be taken. Provisions for data security at the end of a project must be made (see the University of Sheffield’s Good Research Practice Standards, Sections 3.7.2 – 3.7.4: www.shef.ac.uk/content/1/c6/07/20/99/GRPcollated.pdf).

31. The use of confidential information in ways that are consistent with a valid consent will represent no breach of confidence. It may be, however, that there is no valid consent to rely upon and re-contact for fresh consent is not practicable. In such circumstances, only de-identified data can be used unless a researcher is prepared to defend the use of identifiable information for a non-consented purpose as ‘in the public interest’. We would advise any researcher considering this to contact the UREC for further advice.

respected. However, good practice dictates that the child should be encouraged to involve parents or other legal guardians in their healthcare.’ (Paragraph 24)

7 See, for example, General Medical Council advice ‘Consent to Research: Research involving vulnerable adults (paragraphs 21 to 22) (www.gmc-uk.org/guidance/ethical_guidance/6471.asp)

De-identified Data

32. Wherever practicable data should be collected, stored and handled in de-identified forms. Where linkage between datasets is required, e.g. in longitudinal studies, record numbers should be used as far as possible, with special measures used to protect the keys that link such numbers to personal identifiers.

33. Names and addresses are not the only ways of identifying individuals. There are other kinds of information that can be used to identify an individual, for example date of birth, or clinical diagnosis for rare diseases, especially if the area covered by a dataset is small. Similarly the keys for some record numbers, for example NHS number, are relatively easily accessed. Thus while removing name and address provides a ‘first-line’ protection of privacy, identification of the data subject may still be possible.

34. If it is not possible to identify an individual from data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, then those data fall outside of the scope of the DPA 98. Similarly, if an individual cannot be identified from data extracted from confidential information, then use of that de-identified data will not constitute a breach of confidence: a ‘confidence is not breached where the confider’s identity is protected.’ The process of de-identification must, however, be carried out by someone with lawful access to the data in identifiable form.

35. Information can be considered to be de-identified if the means necessary to link the data to a particular individual are both unavailable and are not likely to be made available in the future.

36. Particular care needs to be exercised if control is to be lost over the context within which data may be placed, e.g. through publication, and there is a risk of re-identification by others. This may be particularly the case when dealing with small numbers.

The Deceased

37. While the DPA 98 only applies to the personal data of living persons, the Common Law Duty of Confidence continues beyond an individual’s death. If an individual provided consent to research use of their confidential information before death, then use of their data in terms consistent with the consent given represents no breach of confidence after death. If no valid consent exists, then the justifiability of using confidential information relating to the deceased needs to be assessed (as with confidential information relating to the living in the absence of consent) on a case by case basis.

38. The Department of Health ‘Guidance for Access to Health Records Requests’ (February 2010) offers advice on making such an assessment in the case of health records. We would

---

9. The concern of the law here is to protect the confider's personal privacy. [...] that gives the patient no property in the information and no right to control its use provided only and always that his privacy is not put at risk. [...] In a case involving personal confidences I would hold [...] that the confidence is not breached where the confider's identity is protected.’

10. Department of Health ‘Guidance for Access to Health Records Requests’ (February 2010) also recognises that '[c]urrent legal advice is that the Courts would accept that confidentiality obligations owed by health professionals continue after death. The Department of Health, General Medical Council and other clinical professional bodies have long accepted that the duty of confidentiality continues beyond death and this is reflected in the guidance they produce.’ (paragraph 34)
support that advice (and draw attention in particular to paragraphs 43–45).

**Human Tissue Research**

39. The Human Tissue Act 2004 (the ‘HTA’) provides the framework for the regulation of human tissue research in England, Wales and Northern Ireland. While Human Tissue Research *per se* falls outside the scope of this guidance, research involving human tissue will also, often, involve the processing of confidential patient information. To the extent that Human Tissue Research involves the processing of confidential patient information the law applicable to personal data and confidential information continues to be of relevance.

40. In particular, it should be noted that the law summarised within this guidance remains relevant to confidential patient information associated with ‘existing holdings’. While the consent requirements of the HTA are not retrospective, and it is not necessary to obtain consent under the HTA to store or use an ‘existing holding’ for a scheduled purpose, this does not affect the responsibilities that otherwise and independently exist in relation to confidential patient information. A researcher wishing to use an ‘existing holding’ that is associated with confidential patient information should ensure that the confidential patient information is processed consistent with relevant law.

41. It may be noted that there is a route to ‘special permission’ to enable disclosure of confidential patient information for the purposes of identifying and contacting patients for the purpose of obtaining consent to allow the use of tissue or other samples for medical purposes. Contact either UREC or see the NIGB ECC website for more information.

Research involving human tissue is discussed further in Research Ethics Policy Note No.11: [www.sheffield.ac.uk/ris/other/gov-ethics/ethicspolicy/policy-notes/human-tissue](http://www.sheffield.ac.uk/ris/other/gov-ethics/ethicspolicy/policy-notes/human-tissue)

---

**Additional Guidance: Breaching Confidentiality**

There may be occasions when researchers feel the need to break confidentiality – i.e. deliberately disclose confidential information. For example, this may occur when the researcher becomes aware that the participant is the perpetrator or victim of a crime, or where the researcher feels that the participant is at risk of harm (such as finding out that a participant has a health problem of which they are currently unaware).

It is good practice for researchers to think through the circumstances in which they might be required, or feel they need, to break confidentiality and to have a frank and open discussion about them with participants during the consent process. In thinking through these issues researchers should consider the safety and well-being of participants and also various applicable legal or regulatory frameworks (issues surrounding research involving illegal activities are discussed further in Research Ethics Policy Note No.12: [www.sheffield.ac.uk/ris/other/gov-ethics/ethicspolicy/policy-notes/illegalactivities](http://www.sheffield.ac.uk/ris/other/gov-ethics/ethicspolicy/policy-notes/illegalactivities)).

It is also good practice, depending on the nature of the research, for researchers to inform prospective participants of information that they do not wish to know about, informing them that should they divulge such information then the researcher would be obliged to report it.

---

11 An existing holding is material from the living or deceased that was already held at the time the HTA came into force on 1 September 2006

12 [www.nigb.nhs.uk/ecc](http://www.nigb.nhs.uk/ecc)
The challenge is what to do if an issue emerges that researchers had not expected and had not alerted participants to as part of the consent process. The expectation is that, should such issues emerge, the researcher should always discuss the need to disclose this and seek to obtain the participants’ consent in writing before disclosing it. If the participant does not agree to the issue being disclosed then (providing the disclosure is not a legal requirement) the researcher could provide signposting information to the participant that explains where s/he can obtain advice or support (e.g. a helpline number).

It is worth reflecting, especially when undertaking research with children that a participant may regard the disclosure of particular information as being very sensitive when the researcher may not consider it to be (e.g. a child may regard the disclosure of how many friends s/he has as very sensitive information).

Researchers sometimes risk accidentally disclosing confidential information to people who are not eligible to be informed but there may be understandable, though not justifiable, reasons for doing so including:

- the researcher feels the need to unburden because of the emotionally draining nature of the research (e.g. if the research involves participants discussing experiences that have been difficult or disturbing);
- the researcher seeks professional advice.

Additional Guidance: Disguising the identity of individuals and the implications that anonymisation might have on the research data

The Social Research Association recommends that where researchers need to disguise the identities of participants (e.g. by changing their gender, age, changing a disability from one type to another etc.) in order to protect their anonymity, then the researchers need to carefully weigh up the potential damage to the research data that results from the disguise versus the potential harm to the participant should s/he be identifiable because a disguise was not used. Harm to participants should be avoided but it is also important that the integrity of research results should not be called into doubt due to the use of disguises.

Sometimes, faced with this dilemma, researchers may feel it necessary to avoid publication or to omit certain aspects of their research data or omit individual cases in order to protect the participants. Researchers should take care not to promise participants a level of confidentiality and/or anonymity which they may later find they are unable to meet without jeopardising the research itself, and should think carefully in advance about their plans for the analysis, publication and dissemination of the research findings - complete confidentiality/anonymity is often very difficult to ensure.

Additional Guidance: Conducting Research Surveys

Although some research surveys collect anonymous data that cannot be linked back to individuals, it is worth bearing in mind the requirements of the Data Protection Act 1998 (DPA) when designing a survey form. Although the information may be anonymous when collected, the DPA allows for the possibility that further information could be received that enables the researcher to link information back to an individual. Therefore, it is sensible to incorporate the main requirements of the DPA into a survey form.

The DPA requires that when collecting any form of personal data a fair “Collection Notice” should be given that provides the following information:

(i) The data controller’s identity (e.g. ‘x’ academic department at the University):
(ii) The purpose(s) for which the data is being collected;
(iii) Any further information that is necessary to make use of the data (e.g. third parties to whom you may be passing the data).

Survey forms collecting data should provide the above Collection Notice-prescribed information. This will ensure that participants (i.e. the survey recipients in this case) have been given sufficient information about the research, to obtain consent to collect and use their data. Consent can then be obtained in an appropriate manner (written or verbal).

When choosing questions to include in a research survey the researcher should consider that the data is being collected for a specific piece of research, and the information requested should be adequate, relevant and not excessive. For example, if conducting research into obesity, it may not be relevant to ask about the participant’s political opinions or religious beliefs.