The University of Sheffield
Research Ethics Policy Note no. 4

PRINCIPLES OF ANONYMITY, CONFIDENTIALITY AND DATA PROTECTION

For a detailed discussion of the law on which University policy in this respect rests, see the Specialist Research Ethics Guidance Paper, 'Principles of anonymity, confidentiality and data protection', of which the following is no more than a brief summary.

A researcher who processes (collects, stores, uses, discloses or destroys) identifiable personal information - as defined as in the next paragraph - about living individuals, must comply with the requirements of the relevant data protection legislation, and the Common Law Duty of Confidentiality. A researcher who processes identifiable personal information about deceased individuals, must still consider the requirements of the Common Law Duty of Confidentiality. The processing of robustly anonymised personal information, whether relating to the living or the deceased, falls outside the scope of these legal requirements.

Data protection legislation applies to 'personal data'. This is defined in the General Data Protection Regulation (GDPR) as 'any information relating to an identified or identifiable natural (living) person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.

According to data protection legislation, any processing of personal data must have a defined 'Data Controller' in place (the organisation which determines the purposes and means of processing personal data). For research undertaken by staff or students of the University of Sheffield, the Data Controller will usually be the University of Sheffield (i.e. not a particular individual or research team). Collaboration with other institutions may result in joint Data Controllers. In practice, in the case of discrete research projects, it is highly unlikely that members of the research team will come into contact with data from other parts of the University that may result in the re-identification of participants whose data has been anonymised. However, researchers should think carefully about this possibility when seeking to anonymise their data; strictly speaking, if there is any possibility that anonymised data could be traced back to the individual who provided it via any other data held by, or likely to come into the possession of, the Data Controller, then the data has in fact only been 'pseudonymised'. This means that it would in fact still be classed as personal data. Two examples of situations in which this problem is more likely to arise include:

- administrative research, in which research staff may have access to central University records that may link data to the participants that provided it;
- types of research in which there are particular identifiers that are widely used outside the research team (e.g. health research involving NHS numbers).

The use of identifiable personal information in research should be reduced so far as possible consistent with achievement of the research aims. Thus researchers should always think carefully about (a) whether it is necessary to use identifiable personal information, (b) what is the earliest stage at which de-identification might be possible without compromising the integrity of the research and (c) how full, robust anonymisation can be achieved. All uses of personal information should be defensible as accurate, relevant and not excessive.

If it is necessary to use identifiable personal information, then an appropriate legal basis for the

processing of this data must be identified. The University's view is that for the vast majority of research undertaken at the University, this will bethat 'processing is necessary for the performance of a task carried out in the public interest'. This is set out in the University's Privacy Notice: https://www.sheffield.ac.uk/govern/data-protection/privacy/general.

Providing 'consent' is not being used as the legal basis for processing personal data, it may be possible to use personal data without consent - when the material is already in the public domain, for example. However, from an ethical perspective, consent is still to be preferred, unless it can be shown to be inappropriate for some reason. If a researcher intends to process data without consent, then further advice should be sought.

When gathering identifiable personal information researchers should aim at all times to ensure that its processing is defensible as 'fair, lawful and undertaken in a transparent manner'. This requires that the participant be provided with appropriate information about the uses to which data will be put and any risks that might be involved. Further information can be found in Research Ethics Policy Note no. 2 'Principles of Consent'.

Personal information must be kept secure at all times. The level of security should be proportionate to the risks inherent in the nature of the data, but all personal information should be kept securely e.g. portable devices should be encrypted. Personal information should not be retained for longer than necessary. However, it is recognised that research may require the retention of data for long periods and that this may be justified, for example due to funder requirements. The participant should be given full information about how their data will be used, how it will be stored and for how long (if the latter is not possible, then the participant should be informed of the criteria that will be used to determine retention periods.)

Personal data that are processed for research purposes may be exempt from a GDPR subject-access request. In general, the disclosure of identifiable information, including information that may be identifiable to others, should be avoided 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 individuals involved.

Finally, the Common Law Duty of Confidentiality applies to research, as to all other activities. Individuals have a reasonable expectation of privacy with respect to confidential information that refers to them. Any use of such confidential information that exceeds that which an ordinary person could reasonably be said to expect constitutes a breach of confidence.

For further discussion, including information regarding the additional requirements applying to the collection and use of 'Special Categories' of personal data, see the separate Specialist Research Ethics Guidance Paper entitled: 'Principles of anonymity, confidentiality and data protection'.

NB. The University has a separate policy covering the transfer of research data which relates to human participants between Principal Investigators within the University of Sheffield.