Research Guidance Note 6
Confidentiality, anonymity and data protection

Confidentiality and anonymity

While anonymity and data confidentiality are often used almost interchangeably, they are distinct:

- **Anonymity** means that the participant cannot be identified by anyone (including the researcher).
- **Confidentiality** means that the participant can be identified by the researcher but access to this information will not go beyond the researcher.

Maintaining the anonymity or confidentiality of research data offers advantages to both the researcher and participant. These include:

- To improve the quality and honesty of responses.
- To encourage participation in the study and improve representativeness of the sample.
- To protect the participants' privacy.
- To protect participants from discrimination or other adverse consequences of disclosure.

The principles of anonymity and data confidentiality should be made clear as part of gaining a participant's informed consent. The researcher must make it clear what is to be done with the data they collect and how the individual's identity will be protected.

The research should also explain if there are any plans for the anonymised data sets to be made available to other researchers, in line with the University's Research Data Management policy which encourages such use, sharing and publication as appropriate to ensure the maximum benefit is derived from any research undertaken under its auspices.

The Data Protection Act 1998

The Data Protection Act sets out eight principles governing the use of personal information. The main purpose of these principles is to protect the interests of the individuals whose personal data is being processed by the University and they apply to everything the University does with personal data, unless an exemption applies. The DPA 1998 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.

Respect for confidentiality is essential to maintain trust between the public and those engaged in research. All researchers intending to use personal data must comply with the requirements of the eight principles, the University's Data Protection Code of Practice and in particular sections 5, 6, 7, 8, 11 and 20 and any associated guidance. In addition to computerised records these requirements apply to written records held in a structured filing system, digital and microfiche records, images and video recordings.

The eight principles are that personal data must be:

1. fairly and lawfully processed
2. processed for limited purposes
3. adequate, relevant and not excessive
4. accurate and up-to-date
5. not kept for longer than is necessary
6. processed in line with individuals' rights
7. kept secure
8. not transferred to other countries without adequate protection.

What to consider when using personal data for research

Researchers should always consider when planning a project, giving data to and receiving it from others and before publishing information, whether their research data may lead to the identification of individuals or very small groups. There are two options:

a) comply with the DPA 1998; or

b) anonymise the data to be used so that it no longer falls within the Act's definition of personal data.

Option a) means that all the requirements of the DPA 1998 must be met and option b) means that the personal data to be used must be completely anonymised. This will only be achieved if it is impossible to identify the subjects from that information together with any other information that the University holds or is likely to hold. Researchers are advised to use unlinked and truly anonymised data but if this is not possible, the amount of personal data they use and store should be kept to the minimum necessary to achieve the purpose of the study. Sharing of data should be limited to those who have a demonstrable need to know as part of their role in the research project.

Detailed guidance can be found in the University's Data Protection Code of Practice[18] as well as in a Researcher's checklist[19].

The UK ICO's Code on Anonymisation[20] has recently been published. Appendix 2, Annexes 1 and 2 give some very useful, practical guidance for researchers on how to anonymise research data.

18 Edinburgh Napier University 'Data Protection Code of Practice' (2012). Available at http://staff.napier.ac.uk/services/secretary/governance/DataProtection/Documents/CoP/Code%20of%20Practice%20Revised%20 April%202012.pdf [last accessed December 2015]

19 Edinburgh Napier University 'Researcher's Checklist for compliance with the Data Protection Act. Available at http://staff.napier.ac.uk/services/secretary/governance/DataProtection/Documents/Researcher%27s%20checklist%20revised%20March%202012.pdf [last accessed December 2015]

20 The UK Information Commissioner's Office 'Anonymisation: managing data protection risk Code of Practice' (2012). Available at http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Practical_application/anonymisation_code.ashx [last accessed December 2015]