Research Ethics and Data Protection Briefing Note

Data protection is an ethical issue. It involves respect for individuals and their rights regarding privacy and the use of information about them. External funders, particularly the EU, are seeking increasing levels of assurance with regard to data protection and ethics. Data protection issues are raised formally during the ethics process. However, it is helpful to think about them at the outset of your project as they might affect its timing, design or scope.

This briefing note highlights the following issues of particular importance and should be read in conjunction with the webpages listed at the bottom of this note:

Definition of personal data	Personal data is any information about a living individual who can be identified either directly from the data or by combining your data with other available information.
Consent	You should seek explicit, informed consent to use personal data in research. If you do not have consent, you must justify this in your ethics proposal, and explain what other measures you have built into the project in the absence of consent.
Transparency	As a minimum, you should ensure that research data subjects receive the following information: what information you hold about them; how you will use that information; whether you disclose the information to other organisations (and which ones); whether you combine that information with other data; Whether the data will be held, accessed or used outside the European Economic Area (EEA). If you cannot provide this to research data subjects, you must justify this in your ethics proposal and explain what other measures you have taken, such as publishing a statement covering this information.
Anonymisation	You should handle the least amount of personally identifiable data possible. Can you anonymise the dataset for everyday use? If not, you will need to explain why in your ethics proposal.
Physical and IT security	You should take physical and information security measures appropriate to the risk level of the personal data. Personal data on mobile devices must be encrypted.
Written procedures	You should have written procedures setting out how the personal data is to be handled, stored and accessed.
Training	Staff handling personal data must receive training in their obligations as regards the handling and use of your research data. Details of the various training courses organised by Records Management can be found at: www.ed.ac.uk/records-management/training/current-training-programme/training-course-list It is also essential that Information Security awareness training is undertaken. This can be found at: www.ed.ac.uk/infosec
Passing data to third parties	You should only pass personal data to third parties if you have a written agreement in place governing the use and security of the information and procedures to ensure the transfer is secure.
Receiving data from third parties	If you are using data from another organisation or harvested from the Internet, you must confirm that the use in your research is compatible with what the data subjects were told would happen to the data. For example, Twitter users are told that their public tweets will be used for research; Facebook users are told that their posts will not be collected using automated means.

For more indepth advice, see the Records Management and Information Security websites.