Data Protection in Research

The University must comply with the Data Protection Act 1998 (DPA), which requires that data is collected and used fairly, stored safely and not processed unlawfully. The DPA sets out the Data Protection Principles. In summary, these state that personal data shall:

1. be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met;
2. be obtained for specified and lawful purposes and shall not be processed in any manner incompatible with those purposes;
3. be adequate, relevant and not excessive for those purposes;
4. be accurate and kept up to date;
5. not be kept for longer than is necessary for those purposes;
6. be processed in accordance with the data subject's rights under the DPA;
7. be kept safe from unauthorised access and processing, and accidental loss, damage or destruction;
8. not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

The DPA applies to **personal** *data*, i.e. data which could **identify** a **living individual**. The DPA does not apply to information about deceased people, but you may still owe a duty of confidentiality after death. If data is permanently anonymised so that individuals can no longer be identified it is not subject to the DPA.

Data collected may be in any form, e.g. paper-based records, computer records, audio or visual recordings. For all research where identifiable data will be collected from participants, the researcher must provide adequate assurance through the research ethics process that the research will comply with the DPA.

In order for research to comply with the DPA it must:

1. Provide information to research participants detailing how their data will be used. This is usually in the form of a Participant Information Sheet, and should contain:
    a. Who will have access to the data and how it will be held
    b. The purpose of the data processing
    c. Any potential disclosure of the data
    d. How long the data will be kept
2. Gain consent from participants for collection of their data
3. Have a clear purpose for all data collected
4. Maintain confidentiality of data and protect the identity of individuals
5. Ensure that data is accurate and up to date
6. Hold all data securely:
    a. Physical security measures e.g. locked rooms/cabinets
    b. Digital data security e.g. Password Protection, encryption, virus protection, back-up processes, suitable disposal of IT equipment
    c. Transfers between project sites must be to facilities that comply with the DPA standard

For research involving collaborations outside of the EEA, data may not be transferred to countries unless:

- The country has adequate data protection regulations
- Explicit consent has been gained from participants for overseas transfer of data
- A contract has been signed by the data recipient specifying data protection requirements that must be upheld