Guidance note: Use of personal data in research

1.1 Introduction

This guidance note provides information and advice for employees and students of the University to ensure they use personal data for research with due regard for their participants' rights.

The use of personal data in research is governed by data protection law, which includes the Data Protection Act 2018, and the General Data Protection Regulation.

1.2 Conditions

Personal data may be used in research as long as the following conditions apply:

> The data are not used in a way which causes substantial damage or distress to an individual;
>
> The data are not used to support decisions or measures relating to particular individuals.

1.3 Consent and ethics approval

The University's Code of Research Ethics requires the consent of participants before their personal data are used, except where such consent would invalidate the research.

Where the intent is to use personal data in a research project, the researcher must request research ethics approval through the BREO application.

Please refer to your College's intranet pages for further information.

1.4 Exemptions and exceptions

There are several exemptions and exceptions from the data protection principles when using personal data in research.

> As long as the data are used **only** for research purposes, they can be used for research projects other than the one for which the data were originally obtained.
>
> The data can be held as long as required, although it is expected that they would be *pseudonymised* or *anonymised* as soon as practicable.

If the data can no longer be attributed to a particular individual, the participants cannot exercise their right of access to the data. Upon publication, the research results must also be pseudonymised or anonymised for this exemption be apply.

The data are also exempt from the participants' rights to rectification, restriction of processing, and objection.

1.5 Special category data

When intending to use special category data for research, it is a requirement to obtain *written consent* from the participant. Until the data have been anonymised, you must retain the consent form, to prove that consent was provided.

Special category data includes:

Racial or ethnic origin

Political opinions

Religious or philosophical beliefs

Trade union membership

Genetic data

Biometric data

Health

Sex life or sexual orientation

Alleged commission of offences

Proceedings for an offence committed or alleged to have been committed or the disposal of such proceedings, including sentencing.

Regardless of what kind of personal data you use, you must still comply with the data protection principles, including data minimisation and keeping the data secure.

2 Practical application

2.1 Participant identification

Unless you plan to attribute the data to particular individuals, it is recommended that you assign each participant a code of some kind. The participants' names and other details, and the code which has been assigned, should be kept in a ***separate file*** from the actual data collected for the research project.

The research data should then only use the code to differentiate data from different participants.

2.2 Storage of the participant identification file

The identification file should be accessible to the principal investigator, and as *few* other people as possible who are involved in the project. *It should also be kept separately from the research data*. If it is kept electronically, it should at a minimum be password protected, and that password should not be the same as any password used for the research data file(s).

Under no circumstances should the participant identification file be stored on

3 Pseudonymisation/anonymisation