

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 to 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 unencrypted removable media (laptop or USB (flash) drive).

2.3 Storage of research data

Until the data have been anonymised, they are still considered to be personal data. As with the participant identification file, the data must be securely stored, with appropriate password protection and limited access.

If you need server space in which to store the research data, please contact computing-support@brunel.ac.uk.

2.4 Focus groups

If you have organised a focus group, and intend to produce an audio recording, you should consider providing the participants with aliases to be used during the session(s).

2.5 Sharing research data

In the event that you are working on a project with researchers at other locations, there should in most cases be no need to share the participant identification file. If you decide that it is necessary to do this, you should ensure that you note the reasons, the identity of the person with whom the file was shared, and the date this occurred. Regardless of how you send the file (whether by e-mail or courier), please ensure you obtain a positive indication that the file has been received.

Do not send participant identification files by normal post.

Any research data may be securely shared by using [OneDrive](#).

2.6 Retention

The participant identification file should be retained for as long as the associated research data are retained. If you send your research data to a central archive (such as the UK Data Archive), then you should ensure that you specify under what circumstances (if any) the participant identification file should be disclosed.

3 Pseudonymisation/anonymisation

These are two techniques for removing identifying information in your research data, and increasing the security of the data. There are differences, though.

3.1 Pseudonymisation

The General Data Protection Regulation defines pseudonymisation as: "...the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."

Pseudonymisation is a security measure, but it does not change the status of the data: it will still be personal data.

3.2 Anonymisation

Anonymous data is: '...anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.'

Data that has been rendered truly anonymous is no longer considered to be personal data. This reduces the risk of a data breach and benefits your participants.

However, you cannot say you have anonymised the data unless the possibility of re-identification is extremely small.

The Information Commissioner's Office has published an [Anonymisation Code of Practice](#), which provides background and advice on effective methods of anonymisation. The document references the previous data protection law, but is still an excellent resource.

4 References

Data Protection Act 2018: <http://www.legislation.gov.uk/ukpga/2018/12/contents>

Information Commissioner's Office: ico.org.uk

Guide to the General Data Protection Regulation: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/>

Research Data Management: <https://intra.brunel.ac.uk/s/RSDO/Proposals/Developing-your-Proposal/DataManagement/Pages/default.aspx>