THE UNIVERSITY *of* EDINBURGH

GDPR & Ethical Research

Practical Research Ethics

Hugh Rabagliati

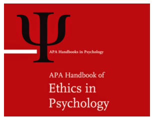
Department of Psychology
The University of Edinburgh

AY 2021-2022

Principles-based research ethics

the british psychological society
promoting excellence in psychology

BPS Code of Human Research Ethics



APA Handbooks in Psychology

APA Handbook of Ethics in Psychology

British Psychological Society

- Respect for the autonomy and dignity of persons
- Social responsibility
- Maximising benefit and minimising harm
- Scientific value

American Psychological Association

- Respect for persons and autonomy
- Justice
- Trust
- Beneficence and nonmaleficence
- Fidelity and Scientific Integrity

Managing your data under the General Data Protection Regulations

What is GDPR?

General Data Protection Regulations

- A set of EU regulations on how individuals and organizations collect and process concerning people.
- World's strictest privacy standards.
- Post-Brexit, subsumed into UK law as the Data Protection Act 2018.
- If an organization wants to work with an EU partner, it must follow GDPR.

Different types of data under GDPR

Data

- Any information collected about or from an individual (e.g., a response time).

Personal Data

- Information about an individual that allows them to be identified (e.g., a name).

Sensitive Personal Data

- Information about an individual that identifies certain protected characteristics, such as:
  - Race & ethnicity
  - Political opinions
  - Physical or mental health
  - and more...

Why are data types important?

Collecting different types of data requires different levels of justification

- Providing personal data could risk the privacy of your participant.
  - But as a *reseacher* you have a legal justification to collect that data, and become its controller.

- Providing sensitive personal data could put your participants at *risk*.
  - Thus, you must have a significant research justification for collecting that data.

Key implication: Only collect the data that you really need, and ensure that that data is kept securely.

What does it mean to keep data secure?

Stored in a GDPR-approved location

- For physical data: A locked filing cabinet in a locked room in your supervisor's laboratory.
- For electronic data: Your University OneDrive account, or within a password-protected Microsoft Teams group with your supervisor and collaborators.
  - *Not* in your personal dropbox or Google accounts.

Locked with protective passwords

- Never leave personal data open. Make sure your laptop has a password. Don't bring printouts to a cafe.

Make data non-personal

- *Anonymize* your data by removing identifying information. Anonymized data can be safely shared.
- Remember, identifying information can be subtle, like a University s-number.

Data subject rights

Personal data that you collect is not strictly *yours.* It belongs to the subject collected from, and they have certain rights.

- **Right to be forgotten.** Subjects can request their data be erased.
- **Right to object.** Subjects can object to how their data is used.
- **Right to restrict processing.** Subjects can stop you processing their data.

And more, see university data policy

Practical implications

1. Plan for your data.

Consider what data, personal data, and sensitive personal data you need to collect. You will need to justify this when you apply for ethical approval in a Data Protection Impact Assessment (DPIA).

2. Design your consent form right

The PPLS ethics portal contains example consent forms that will help you appropriately tell participants what data you will collect, and how they can contact you.

3. Plan for data storage

Remember that you need secure and flexible storage, that will allow you to safely secure sensitive data, and process it when needed.