DATA PROTECTION AND STORAGE GUIDANCE FOR RESEARCHERS

Version:	1.1
Owner:	Deputy University Secretary
Approved by:	GDPR Project Board
Approval date:	May 2018 Minor Revisions August 2018
Review due date:	May 2020
Version history:	New document

Data Protection Guidance for Researchers

Contents

1. Introduction 1
2. Data controllers/processors and collaborations 2
3. Exemptions and appropriate safeguards for research data 2
4. Data subject rights 2
5. Automated decision-making 3
6. Personal data breaches 3
7. Defining personal data 3
8. Defining processing 4
9. Training and sources of information 4
10. Seeking approval for research projects using personal data 5
11. Retention of personal data 5
12. Legal basis 5
13. Providing information 6
14. Providing information verbally 8
15. Re-using research participant data 8
16. Transferring research data with employment 8
17. Project design and data security 9
18. Transferring data outside of the EU 11

1. Introduction

This guidance has been prepared and approved in response to the General Data Protection Regulation and the UK Data Protection Act 2018. This is a living document, and may be updated from time to time as the legal and regulatory environment evolves. This document should be read in conjunction with the University's Data Protection Policy.

A separate notice setting out transition arrangements and how this information should be applied to existing projects is available here.

GDPR applies to personal data of EU citizens regardless of where the processing takes place, and to non-EU citizens where the personal data is being processed in the EU. This guidance applies to all staff and students who undertake research at the University, including scientific, historical and statistical research.

The University is committed to providing the necessary resources, training and guidance to facilitate research. All researchers are expected to comply with this guidance and all other policies, procedures and guidance relating to data protection.

The guidance does not cover ethical issues, and researchers are still expected to comply with the University's Research Ethics Guidelines.

The guidance is supported by the following documents:

- Research Participant Privacy Notice
- Participant Consent Form Template
- Research Participant Information Sheet for indirectly collected or re-used personal data
- The University's Ethics Application Form

2. Data controllers/processors and collaborations

For research projects based at the University, the University will most likely be the data controller. It doesn't make a difference if the project is taking place in a country outside the UK or the EEA.

Where the University and a third party are collaborating on a research project, both the University and the third party are likely to be data controllers. If this is the case, an agreement should be in place between the University and the third party setting out their respective responsibilities for compliance with data protection legislation. If you are collaborating with a third party, you should approach the Research Office for guidance on producing a written agreement.

If the University is not the data controller (for example, where work is being performed on behalf of another party who determines the means and purpose of processing), the data protection obligations will still apply to the University as a data processor. This would mean that the University will be responsible for ensuring the security of the data and for keeping records of processing activities.

Data protection legislation does not apply to anonymised data, and so if collaborations are taking place between institutions, including those outside of the European Union, it may be more straightforward to anonymise the research data. Anonymisation must conform to the standards set out in Section 17 of this guidance. If personal data is pseudonymised in accordance with Section 17 of this guidance, then it is acceptable to send the pseudonymised data file, which does not contain any personal data, to the other institution without producing a written agreement.

3. Exemptions and appropriate safeguards for research data

There are a number of exemptions for research under data protection legislation. These exemptions have been incorporated into this guidance. However, the exemptions only apply where appropriate safeguards have been taken to protect the personal data. Information about the required safeguards is set out in Section 17 of this guidance. This guidance must be followed by all researchers. Furthermore, in accordance with accepted ethical standards, research participants should not generally be named in any published materials.

4. Data subject rights

Research participants have a general right to opt-out of further processing. If they do opt-out, there is no need to delete their research data but it should normally only be used in an anonymised form or as part of an aggregated data set.

GDPR also grants individuals other rights in relation to their personal data, including the right to access the data, the right to object to processing, the right to request that the data be deleted (the right to be forgotten), the right to request that the processing of the data be restricted and the right to request the rectification of inaccurate or incomplete data.

These rights are not absolute, and the University considers that they do not apply where personal data is being processed for the purposes of research. If a research participant requests a copy of their personal data, researchers may provide this but are under no obligation to do so.

Any queries about research participants exercising their rights as data subjects should be directed towards the Research Office.

5. Automated decision-making

All data subjects, including research participants, have the right not to be subject to a decision based solely on automated decision-making, including profiling, which produces legal effects concerning or substantially affecting that individual. This is unlikely to be an issue for researchers, but may arise in some circumstances. If this is relevant to your research, then you should seek advice from the Research Office.

6. Personal data breaches

If a researcher experiences or suspects a personal data breach, they should notify their line manager and the University's Data Protection Officer immediately. Research students should notify their supervisor, who should notify their line manager and the Data Protection Officer immediately. The researcher should also notify any partner organisations of the breach.

The sooner a breach is reported, the more likely it is that it can be contained and any damage can be minimised. The University is required to inform the Information Commissioner's Office (ICO) of certain types of breaches within 72 hours. There will be significant fines for organisations who fail to report personal data breaches.

7. Defining personal data

'Personal Data' is defined as, "Any information relating to an identified or identifiable person (a 'data subject) or from which a person can be identified either directly or indirectly." Examples of personal data include:

- Name
- Age
- Address
- Height
- Weight

Personal data includes an expression of an opinion about a person, or the opinion of that person if it is possible to use this to identify them. This may include, for example, interview responses or questionnaire material. The operative question is whether an individual can be identified, either directly or indirectly, by the data.

If as part of a research dataset you have two or more separate categories which, when combined, could be used to identify a person, then you should treat each of these categories of data as personal data.

There are a number of types of personal data defined in the relevant legislation as 'special categories of personal data'. Special categories of personal data include the following:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Health
- Sex life
- Sexual orientation
- Biometric data
- Genetic data
- Criminal convictions data

Generally speaking, additional care should be taken when processing special categories of personal data.

This guidance applies to all research that uses personal data, including special categories of personal data.

8. Defining processing

Processing is defined as any operation or set of operations which is performed on personal data or on sets of personal data. This includes, but is not limited to the collection, recording, organisation, storage, alteration, use or disclosure of personal data, or otherwise making personal data available. Almost any research project that involves participants will involve processing personal data.

9. Training and sources of information

All staff and postgraduate research students are expected to complete data protection training as part of their induction, and refresh the training on a regular basis. Undergraduate and postgraduate taught students involved in research will be provided with alternative training. If you are a member of staff and have not completed the training, then you should contact Human Resources. If you are a research student and have not completed the training, you should contact your research supervisor. Further specific guidance regarding data protection for research can be accessed from the Research Office.

10. Seeking approval for research projects using personal data

Given the University's responsibilities as data controller/processor, it is essential that adequate governance arrangements are in place to ensure that personal data is used properly during the course of research. Any researcher using personal data as part of a research project should complete the University's Ethics Application Form. In most cases, this will be a simple and straightforward exercise. The aim is not to cause an additional administrative burden, but rather to ensure that any risks relating to data protection are highlighted at an early stage and can be appropriately managed.

11. Retention of personal data

GDPR does not say specifically how long personal data should be held for. However, an underlying principle is that personal data is not held for longer than is necessary. In all cases, research participants should be informed how long their data will be held for at the beginning of the project. The University has published a Record Retention Schedule, which sets out the amount of time different types of data will normally be kept for, and contains provisions relating to research data. Anonymised data can be held indefinitely, and so consideration should be given as to whether the same aims can be achieved by anonymising the data.

12. Legal basis

It is essential that any personal data used as part of a research project is only processed where there is a clear legal basis to do so. Where data is being processed unlawfully, it is likely that the processing will need to stop and the data will need to be deleted.

Processing carried out in the public interest

Personal data processing for research purposes is normally carried out by the University in the public interest, which means that consent from research participants to process personal data is not required. This is separate from ethical consent to participate in a research project, and means that if a research participant withdraws from the study (i.e. withdraws ethical consent), they are not automatically entitled to have their personal data deleted.

In order to rely on the public interest as an appropriate legal basis, a researcher must be able to demonstrate that the research methodology represents a targeted and proportionate way of achieving the research aims. This means that there should not be another reasonable and less intrusive way of achieving the same result.

A research participant can request that their personal data is erased, but there is no obligation to do so if erasure is likely to render impossible or seriously impair the achievement of the research objectives. In determining whether this is the case, researchers should consider whether the same results could be achieved by anonymising the data (see Section 17 below).

Legitimate Interests

Legitimate interests may be the appropriate legal basis where it would be difficult to demonstrate that the research was necessary to meet a public interest, for example,

because the research was commercial in nature or funded by a private company. In determining whether or not you can use legitimate interests as your legal basis, you should undertake a three step assessment:

- Identify the legitimate interest (further guidance available from Research Office)
- Consider whether the processing of personal data is necessary to meet those interests
- Determine whether those interests are outweighed by the rights and interests of the research participants

The ICO recommends that those considering this basis should undertake a Legitimate Interests Assessment (LIA), comprising three parts. The first part involves identifying the legitimate interests in question; the second determining whether the processing of personal data is necessary to meet those interests; and the third determining whether those interests are outweighed by the rights and interests of the research participants. Section 6 of the Research Ethics Application Form contains instructions for completing an LIA.

Special Category and Criminal Convictions Data

For research involving special category data and criminal convictions data, the legal basis will usually be that the processing is necessary "for archiving purposes in the public interest, scientific or historical research purposes.

Common Law Confidentiality

Separate to data protection legislation is the concept of common law confidentiality, which suggests that if information is given in circumstances where it is expected that a duty of confidence applies, the information cannot normally be disclosed without the information provider's consent. Common law confidentiality often arises in respect of health records, but may arise in other circumstances. Where it arises, researchers will need to gain the consent of research participants before using the information or disclosing it as part of a research project. Common law confidentiality is beyond the scope of this guidance, and researchers should seek advice from the Research Office. However, the NHS has developed a range of materials to support research involving health records, which can be accessed here.

Ethical Consent

As suggested above, this guidance relates specifically to data protection and does not consider research ethics. Regardless of the lawful basis for processing identified above, researchers will need to consider whether it is necessary to obtain ethical consent from research participants before collecting data.

13. Providing information

Data protection legislation requires that data subjects are provided with certain information at the point their personal data is captured. This requirement applies to all research conducted at the University of Roehampton.

If you are collecting personal data from a research participant, they must be provided with the following information:

- Reference to the University's Data Protection Policy
- Confirmation that the University is acting as data controller, and contact details for the Data Protection Officer
- The purpose of the personal data processing (usually the research aims)
- The legal basis on which the processing is conducted (see Section 12)
- Details of any third parties who will have access to the information (including partner institutions or external contributors), or to which the data will be transferred
- Details of any transfers outside the EU, and confirmation of any safeguards that are in place (see Section 18)
- How long the data will be stored for
- Any rights held by the data subject
- The right of the data subject to make a complaint to the Information Commissioner's Office
- Whether personal data will be used for automated decision-making or profiling which significant affects the legal rights of a research participant (see Section 5 below)
- The data subject's right to either opt-out or withdraw their consent

A generic Research Participant Privacy Notice and accompanying model Participant Consent Form have been developed which incorporate these requirements. If you need to use a different form to gather participant consent, you should contact the Research Office to ensure that it is compliant with data protection legislation.

Processing personal data that has not been collected directly from the participant

There may be circumstances where personal data used as part of a research project is not collected directly from the data subject. In such a case, a researcher will need to ensure that the organisation or individual responsible for collecting the data did so lawfully, and was entitled to transfer the data to the University. It is not necessary for the personal data to have been collected for the purposes of research.

If the data has not been collected lawfully, or if the organisation or individual was not entitled to transfer the data to the University, the researcher should inform the Data Protection Officer.

Where personal data has been collected and transferred lawfully, the researcher must provide the research participant with the information outlined above. This information should be provided as soon as possible, and at the latest within one month of receiving the personal data. A model Research Data Information Sheet template has been developed for this purpose.

This requirement does not apply if contacting the data subjects would be impossible or involve disproportionate effort, or it would render impossible or seriously impair the achievements of the research objectives. If the researcher intends to make use of this exemption, they must ensure that appropriate safeguards are in place (see Section 17 of this guidance). They must also make the information that would otherwise be provided to the data subject publicly available. This may involve, for example, publishing a notice on the project's website.

The University will need to provide the above information in situations where is acting as joint personal data controller.

14. Providing information verbally

In certain cases, researchers may not be able to provide written information regarding personal data processing. This may be because of the circumstances of the research project, or because the participant cannot read or write. In such circumstances, it is acceptable for the researcher to provide the necessary information verbally, provided that the participant understands the information and the researcher keeps a clear record that it has been given. It is important to ensure that the participant understands the information that is being given, so depending on the circumstances, this may involve altering or simplifying the information set out in the template information forms described in Section 13. As with all research participants, the researcher will need to ensure that the participant in question has the capacity to consent to the project.

15. Re-using research participant data

Data protection legislation anticipates that researchers will need to use previously collected personal data for additional research, and a specific exemption is included which allows for this. Provided that the original legal basis on which the personal data has been processed is appropriate, the researcher will not need to identify a new legal basis. Where personal data are repurposed, the research participant should be provided with up-to-date information, unless it would be impossible or involve disproportionate effort, or it would render impossible or seriously impair the achievements of the research objectives. The Research Participant Information Sheet for indirectly collected or re-used personal data should be used for this purpose.

16. Transferring research data with employment

Many researchers seek to take their research data with them when they leave their employment at the University, or bring data with them when they enter employment here. The most straightforward way to facilitate this is to anonymise the data in line with the provisions of Section 17 of this guidance. In the event that this is not possible, the following provisions apply:

Transferring research data out

As above, the University is generally the controller of research data processed by researchers who work here. When a researcher leaves the University and takes the research data with them, the data is transferred from the University to either the researcher's new institution or to the researcher as individual data controller. Where this transfer occurs, the new institution or the individual researcher will take responsibility for compliance with data protection legislation.

For a transfer to be permissible, the research participant should be informed at the point their data is collected that this may occur. The generic Research Participant Privacy Notice contains information to this effect.

Transferring research data in

The same principles apply where a new researcher joins the organisation and seeks to bring research data with them. In this situation, the University will usually become the data controller and will therefore assume responsibility for compliance with data protection legislation. The researcher should be able to provide evidence that they are entitled to transfer the personal data, for example in the form of a privacy notice. The researcher should also provide research participants with a link to the University's Research Participant Privacy Notice, unless contacting the data subjects would be impossible or involve disproportionate effort.

17. Project design and data security

As stated at the beginning of this guidance, there are a number of exemptions for research under data protection legislation. These exemptions have been incorporated into the guidance. However, the exemptions only apply where appropriate safeguards have been taken to protect the personal data.

This section sets out information about how personal data can be effectively safeguarded. All researchers are expected to follow this guidance. If the nature of a research project is such that a derogation is required, prior authorisation should be sought via the Ethics Approval Process.

An underlying principle of GDPR is data minimisation, which means that the personal data being processed should be the minimum necessary for the stated aims of the research project. All researchers should therefore consider whether the research aims can be achieved using anonymised personal data. Where this is impossible, researchers are expected to use pseudonymisation as standard.

Anonymous publication

In accordance with accepted ethical standards, research participants should not generally be named in any published materials.

Data Protection by Design

As part of the Ethics Approval Process, you will be asked if the research project is likely to result in high risk to the rights and freedoms of the research participants, specifically with respect to their personal data.

This will depend on the nature of the project and the types of personal data being used. A project is more likely to represent a high risk if:

- It involves a large number of research participants and the use of a high volume of personal data
- It involves the use of special categories of personal data, including health data
- It involves transferring personal data outside of the European Union
- It makes use of non-standard University IT equipment

You may be required to complete an additional data protection impact assessment form, which must be authorised by the Data Protection Officer before the project can commence.

Anonymisation

Anonymisation is where a dataset is edited, with particular fields removed, so that it is not possible to identify a natural person whether on its own, or in combination with other types of data. Anonymisation must be complete and irreversible. If an original copy of the dataset exists, regardless of where it is stored, then the data has not been anonymised.

Researchers should give consideration as to whether personal data contained within the dataset is required to complete the stated aims of the research project. If personal data is not required, and is unlikely to be required in the future, then it should be permanently removed from the dataset at the earliest opportunity.

Data protection legislation does not apply to anonymised data, and so removal of the personal data will give researchers greater flexibility.

Pseudonymisation

Pseudonymisation involves processing personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information. This identifying information, such as a data subject's name, address or date of birth, should be kept separately and stored in such a way as to prevent its use in identifying the data subjects. This might involve storing the identifying information in an encrypted, password protected file which is not circulated amongst the research team. The separate, pseudonymised data can then be shared with greater confidence that no infringement of personal data rights will occur.

Researchers are expected to use pseudonymisation as standard practice.

An example of pseudonymisation is as follows:

Original dataset:

Name	Date of Birth	Pseudonym	Data Type 1	Data Type 2
Aliyah	26/03/1995	#1111	50g	10mm
Ben	19/01/1990	#1112	48g	11mm
Craig	03/08/1985	#1113	52g	6mm
Diana	10/12/1988	#1114	51g	8mm

Pseudonymised dataset:

Personal Data File - Stored securely for reference only		
Name	**Date of Birth**	**Pseudonym**
Aliyah	26/03/1995	#1111
Ben	19/01/1990	#1112
Craig	03/08/1985	#1113

Pseudonymised Data File - Used for research purposes (should not include any personal data)		
Pseudonym	**Data Type 1**	**Data Type 2**
#1111	50g	10mm
#1112	48g	11mm
#1113	52g	6mm

Diana	10/12/1988	#1114	#1114	51g	8mm

In this example, the original dataset is split into two separate sets. Neither set should contain all the data. The only shared field should be the pseudonym. The 'Personal Data' file should be stored securely by the lead researcher in a stable format, either physically or electronically. Copies should not be made, and the lead researcher should carefully control access to the Personal Data file. The 'Pseudonymised Data' file can be used by researchers for processing, analysis and publication, but care should still be taken to ensure data security and integrity. If it is necessary to transfer the entire dataset, then the two files should be transferred separately. If personal data is pseudonymised in this way, then it is acceptable to send the pseudonymised data file, which does not contain any personal data, to external institutions, including those outside of the EU.

Data storage

The University provides high-capacity, secure storage facilities for research data. Researchers are expected to use these facilities to store research data, and should not store personal data on the following:

- Electronic devices, including laptops, phones and tablets that are not password protected and encrypted;
- Portable storage devices, including USB thumb drives and portable hard drives that are not password protected and encrypted;

Current advice on how to password protect your devices and encryption can be accessed from the Helpdesk (helpdesk@roehampton.ac.uk).

Unsecured personal data should not be transmitted via email, either internally or externally. It is acceptable to secure data by:

- Sending password protected information via one means (e.g. email, link share, etc.)
- Then sending the password itself via another means (e.g. SMS, phone call)

It is preferable to share personal data using the University communities (e.g. SharePoint). If you contact the helpdesk, they will facilitate access to a SharePoint community accessible by external parties. Other solutions may be provided in the future and this document will be amended to reflect changes.

Access to sharing and storage resources should be audited and recorded regularly by the project owner, principal investigator or supervisor to ensure that access is reviewed and managed appropriately for the project. Frequency of audits will depend on the sensitivity of the data shared.

18. Transferring data outside of the EU

It will be possible to continue transferring personal data outside of the European Union after the introduction of the GDPR, but only if it can be demonstrated that one of a specific number of safeguards or conditions has been met.

As set out in Section 2, personal data transfers to an external organisation for research purposes should be supported by a written agreement. Researchers should seek advice from the Research Office on such agreements, including when seeking to transfer personal data outside of the European Union.

Generally speaking, transfers outside of the European Union may take place if one of the following conditions has been met:

Adequacy decision

The European Commission has decided that the data protection laws of the following countries are adequate such that personal data may be transferred there:

- Countries in the European Economic Area
- Andorra
- Argentina
- Canada (Commercial Organisations)
- Switzerland
- Faroe Islands
- Guernsey
- Israel
- Isle of Man
- Jersey
- New Zealand
- Uruguay

Transfers can be made to the United States provided that the organisation has been certified under the EU-US Privacy Shield Framework. The list of companies certified under Privacy Shield can be found on the Privacy Shield Website.

Transfer subject to appropriate safeguards

This will involve setting out a specific written agreement with a third party. The Research Office can assist with this process.

Anonymised and pseudonymised data

Data protection legislation does not apply to anonymised data, and so if collaborations are taking place between institutions, including those outside of the European Union, it may be more straightforward to anonymise the research data. Anonymisation must conform to the standards set out in Section 17 of this guidance. If personal data is pseudonymised in accordance with Section 17 of this guidance, then it is acceptable to send the pseudonymised data file, which does not contain any personal data, to the other institution.

Cloud Storage

Please note, many cloud storage services use servers based outside of the European Union. Use of these services would constitute a transfer for the purposes of this section. The University provides a cloud storage service based in the European Union.