

Data management plan

This Data Management Plan ensures that the data created in the research project is managed effectively. This plan aims to define what data is being created, who is responsible for it and how it is going to be stored and made accessible.

1. Summary

1.1	Funding body	
1.2	Any partnership institutions involved	
1.3	Funding (does the funding include data management)	
1.4	Aims of the research:	
1.5	Timescale of the Project:	
1.6	Timescale for the data to be available:	
1.7	Roles and responsibilities:	

2. Data Source

2.1	What kind of data will you be using:	
2.2	What kind of data will you be creating:	
2.3	Quality Assurance of data created:	

3. Legal and ethical issues

3.1	Will there be any ethical issues that may arise from the research data and any relevant committees that must be consulted?	
3.2	Will the research data contain Personal data? (see data protection guidance and checklist below in Appendix A)	
3.3	If so, what provisions are being made to be compliant with data protection legislation?	
3.4	Is there any data that would be exempt if the data was requested under the Freedom of Information Act (see FOIA exemptions below in Appendix B)?	
3.5	What are the intellectual property rights around the data?	

4. Access, data sharing and re-use

4.1	Who is responsible for authorising access to the data?	
4.2	Will there be any access issues around the data?	
4.3	What is the procedure for obtaining access?	

4.4	Are there any embargo periods?	
4.5	Are there any existing data sets in this area of research – how are they stored?	
4.6	If the data is to be shared, how will it be shared?	

5. Metadata

5.1	What contextual details do you need to capture in order to make your data meaningful to users other than the project team?	
5.2	How will this metadata be captured for the purposes of the project?	

6. Storage

6.1	Who is responsible for storing the data?	
6.2	Where and how will the data produced by this project be stored? E.g. paper files, an electronic database	
6.3	What are the backup and security arrangements for the data?	

7. Deposit and long term preservation

7.1	Who is responsible for what happens to the data once the project is completed?	
7.2	Where and how will the data produced by this project be stored once the project is completed?	
7.3	What provision has been made to make data suitable for long term preservation?	
7.4	Is the data being submitted to another institution?	
7.5	Is the data being submitted by another institution(s)	

8. Data Protection Checklist

	Tick where appropriate
I am collecting personal data	
I am collecting special category data	
I am collecting criminal convictions data	
Where I am collecting data directly from individuals, I am explaining clearly what will happen with their data	
I understand the legal basis I am using to process my data	
I understand the concept of 'appropriate safeguards' and how I will apply this to my research	
I am transferring my data outside the EEA and have a plan in place how to this in line with data protection legislation	

For any further information, please contact research services at research.ethics@sas.ac.uk

Version 3 July 2018

APPENDIX A – Data protection guidance

The University is subject to the General Data Protection Regulation and the UK Data Protection Act 2018.

1. Are you collecting personal data?

The definitions of data in the legislation are as follows:

Personal data

- information relating to an identified or identifiable natural person ('data subject');
- individuals can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- applies only to living individuals "this Regulation should not apply to deceased persons"

Special Category data

- personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation

Criminal Convictions data

- personal data relating to criminal convictions and offences or related security measures

If you are collecting any of this type of data, please continue with the checklist. If NO, return to the Data Management Plan.

'Processing' is the term used in data protection legislation around the holding of data. Everything you do with the data from collection to destruction is described as 'processing' by the law.

2. Meeting the data protection principles

The University is required to process personal data according to the following six principles:

Data Protection Principles	The context for research at the University
<i>Lawfulness, fairness and transparency</i>	The researcher explains to their interviewees how they processes personal data at the point of collection and for what purposes. In circumstances where the data is not sourced from the individual, information is made available which explains how the data is used.
<i>Purpose limitation</i>	The researcher only uses the personal data it has for the purposes it was collected for, unless certain safeguards around re-use apply.

<i>Data Minimisation</i>	The researcher only collects personal data which is relevant to the purposes it is required for, unless certain safeguards around re-use apply.
<i>Accuracy</i>	The researcher ensures that the data is correct, up to date and able to be rectify any mistakes quickly
<i>Storage Limitation</i>	The researcher does not retain personal data for longer than it is needed, unless certain safeguards around long term or permanent storage apply.
<i>Integrity and Confidentiality</i>	The researcher protects their personal data against unauthorised access, loss or destruction by a range of security measures.

3. What type of data subjects are you researching?

The data subjects in research will likely fall into two categories:

- Individuals who provide a unique set of data directly (or via a mediator) to the researcher as part of a project, such as an audio interview, a questionnaire or a series of actions that give results (e.g. results from a physical or mental test)
- Individuals whose data is obtained by a researcher from primary source material or secondary literature (e.g. researching a living political figure from contemporary media or biographies, collating public social media handles and statements)

4. What is the legal basis for processing?

The University needs to meet one of the six lawful bases in order to process personal data. The most common for research contexts will be the following:

Legal basis	Examples for a research context
<i>Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller</i>	Research as task carried out in the public interest

The 'participation consent form' is a long established resource for academic researchers taking an ethical approach to working with research participants and should continue to be used. The University does not advise using 'participation consent' as a legal basis for processing personal data.

For special category data, in addition to the original legal basis, the following are most likely to apply:

Legal basis	Examples for a research context
<i>processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes</i>	Collection of data in an interview; Storage and re-use of data in subsequent publications

processing relates to personal data which are manifestly made public by the data subject;

Using primary source material or secondary literature such as published books, newspapers and websites where the individual has a well-defined public political affiliation, sexuality or ethnicity

In regards to criminal convictions data, the University is also required to meet a condition from the UK Data Protection Act 2018. In this case the following is most likely to apply:

Schedule 1 Part 1 “Conditions relating to employment, health and research etc.”

4 Research etc.

This condition is met if the processing—

(a) is necessary for archiving purposes, scientific or historical research purposes or statistical purposes,

(b) is carried out in accordance with Article 89(1) of the GDPR (as supplemented by section 19), and

(c) is in the public interest.

‘In accordance with Article 89’ means that data must be processed with appropriate safeguards and respect for the essence of data protection. ‘In the public interest’ is less definable, but the formal academic environment and educational mission of University research should always be considered to be in the public interest.

If you feel that the legal bases described above do not fit with your research, please discuss with your supervisor and discuss with the Data Protection and Information Compliance Manager.

5. What are ‘Appropriate safeguards’?

The provisions and exemptions to support researchers in GDPR and the UK DPA 2018 do not absolve researchers to manage the personal data of research participants and other living individuals referenced in their research fairly, lawfully and securely. The flexibility around the use of personal data in research must be balanced against the essence of the right to data protection and make suitable and specific measures to safeguard the rights of individuals.

Article 89 (1) of the GDPR states:

Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject.

Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation.

Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner.

Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

Whilst there is no single way to do this defined in the law, the general expectations would be as follows:

<p>How the data is analysed and presented (include reference to this in sections 4 and 7 in the Data Management Plan)</p>	<ul style="list-style-type: none"> • Research does not identify individuals, where this does not affect the purposes of the research • Research does not lead to a decision being made that affects that individual
<p>How the data is stored (include reference to this in section 6 of the Data Management Plan)</p>	<ul style="list-style-type: none"> • Data is, where possible, anonymised or pseudonymised • Data is kept securely to guard against unauthorised access, loss or misuse • The principle of 'data minimisation' is observed • A plan to effectively preserve the data so it does not become obsolete

6. Will you be transferring the data outside the European Economic Area (EEA)?

Transfers outside the European Economic Area potentially problematic for research data, which is often created in projects resulting from international collaboration. A data management plan should ensure that any personal data held outside the EEA is stored to an adequate level of protection. In the US the use of 'Privacy Shield' accreditation or model contractual clauses are sometimes used. Check with any the partner institutions you are carrying out your research with.

7. Further Information

The University's Data Protection Policy <https://london.ac.uk/about-us/how-university-run/policies/data-protection-policy>

The University's data protection officer: data.protection@london.ac.uk

Guidance on data protection and research <https://www.sas.ac.uk/research/research-office/research-ethics>

Information Commissioner's Office - The UK's regulatory body for Freedom of Information, Data Protection and the Environmental Information Regulations. <https://ico.org.uk/>

APPENDIX B – Relevant Freedom of Information Act exemptions – research data

The following is a brief summary of Freedom of Information exemptions that may be relevant to research data. If you received a Freedom of Information Request for your research data please contact the Data Protection and Information Compliance Manager as soon as possible.

1. Exemptions under the Freedom of Information Act

The Freedom of Information Act provides rights of access to information held by public authorities in England, Wales and Northern Ireland. If the University receives a request for information, it needs to provide it within 20 working days. The only information that can be withheld must relate to specific legal exemptions provided within the Act. The following exemptions may be relevant to research data. Some exemptions require a 'public interest test'. This means that, even if the University agrees that the information falls under a specific exemption, it may be in the public interest to disclose it anyway.

Please consult the University Records Manager for any further information on Freedom of Information. You can also view the University's Freedom of Information policy at <https://london.ac.uk/about-us/how-university-run/policies/freedom-information>

1.1 Section 22 - Information intended for future publication

This exemption can only apply when there is a reasonable, planned publication date. It cannot be used if there is no credible intention to publish. The Data Management Plan should include indicative dates for publication if possible. This exemption requires a public interest test.

1.2 Section 36 - Effective conduct of public affairs

This exemption covers the 'free and frank exchange of views' and other discussions relevant to research projects. However, this exemption is subject to many variable factors such as the timing of the request and the nature of the research data. This exemption requires the authorisation of the Vice-Chancellor and is subject to the public interest test.

1.3 Section 40 - Personal information

If the research data contains personal information, as discussed above in Appendix A, then this information is likely to exempt from disclosure under the Freedom of Information Act. This exemption does not require a public interest test.

1.4 Section 41 - Information provided in confidence

The University can argue that information is exempt from disclosure if it has been 'provided in confidence'. This exemption can be applied only to information obtained by the University from another party; not for information created by the University. The University would also need to demonstrate that disclosure would result in an 'actionable breach of confidence', where the provider of the information could take the University to court and be likely to be successful. This exemption does not require a conventional FOIA public interest test, though there are public interest arguments in considering whether the information is confidential.

1.5 Section 43 - Commercial interests

Information can be exempt if its disclosure would or would be likely to prejudice the commercial interests of any person, including the University. Research is often carried out in a competitive commercial climate and commercial interests may be relevant in withholding a request for research data. This exemption requires a public interest test.

2. Grounds for refusal

There are two relevant sections of the Act which provide the University with grounds to refuse requests.

2.1 Section 12 - Appropriate limits

Section 12 of the Freedom of Information Act, 'Exemption where cost of compliance exceeds appropriate limit' allows the University to refuse a request for information if it estimates that meeting the request would exceed the appropriate cost limit. The appropriate limit currently equates to 2½ days' work (18 hours) at a rate of £25 per hour. In the event of a request being estimated to exceed appropriate limits, the University will first seek to narrow down the request with the requester in order to provide relevant and useful information within the limit. If the requester refuses to do this then the request will be either refused outright or a fees notice issued.

2.2 Section 14 - Vexatious requests

Section 14 (1) of the Freedom of Information Act states that public authorities do not have to comply with vexatious requests. The Information Commissioner considers repeat requests, requests in such numbers that resources will be diverted and requests of no serious purpose as potentially vexatious. The University will assess vexatious requests in line with the guidance provided by the Information Commissioner.