Guidance for Researchers on Appropriate Safeguards under the General Data Protection Regulation 2016 (GDPR) and the Data Protection Act 2018 (DPA)

A. Introduction

This guidance note, designed to be read in conjunction with UCL's 'Guidance for Researchers on the Implications of the General Data Protection Regulation and the Data Protection Act 2018' (**Original Guidance**), provides further information on the 'appropriate safeguards' that must be put in place where either:

- **personal data;**
- **special categories of personal data**; or
- personal data relating to **criminal convictions or offences**,

are processed at UCL in a research context.

This document was last updated on 8 November 2018. It may be updated further as relevant guidance on the issues raised is published by the UK Information Commissioner's Office (**ICO**).

B. Definitions

Personal data means any information relating to an identified or identifiable living individual. The definition of personal data in law is broad and covers direct identifiers (like a person's name) and indirect identifiers (like a full postcode). An **identifiable individual** is one who 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'*
>
> [GDPR, Article 4]

Pseudonymised personal data means:

> *'…**personal data** [that] 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'*
>
> [GDPR, Article 4]

Anonymised data is data which does not relate to an identified or identifiable natural person or personal data that has been rendered anonymous in such a manner that the data subject is not or no longer identifiable.

Special categories of personal data means:

> *'…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'

[GDPR, Article 9]

C. Scope

Like our Original Guidance, this guidance applies only to researchers who are processing **personal data** as defined above.

If you are processing **anonymised data** as part of your research, this guidance does not apply to your work.

If you are processing **pseudonymised personal data** as part of your research, then this guidance applies to your work.

D. What are the requirements relating to 'appropriate safeguards' in data protection legislation?

Under data protection legislation, 'appropriate safeguards' must be put in place where personal data is processed for research purposes. This is important because if these safeguards are not put in place, then researchers cannot benefit from a series of research-specific exemptions from powerful individual rights that could significantly impair their research project. This is explained further in (iv) below.

This section will explain the requirements relating to appropriate safeguards in further detail.

(i) Background: legal basis for processing personal data in a research context

Researchers at UCL should generally rely on the following as their legal bases for processing:

- **all personal data:** Article 6(1)(e) of the GDPR , i.e. the 'public task' basis. For further information on this, please see UCL's Statement of Tasks in the Public Interest here;
- **special category data:** Article 9(2)(j) of the GDPR and Schedule 1, paragraph 4 of the DPA 2018, ie for research purposes; and
- **personal data relating to criminal convictions or offences:** Article 10 GDPR and Schedule 1, paragraph 4 of the DPA 2018, ie for research purposes.

Where the 'research purposes' basis is used, the processing must be:

- necessary for archiving purposes in the public interest, **scientific or historical research purposes** or statistical purposes;
- carried out in accordance with **Article 89(1) of the GDPR**, as supplemented by **section 19 DPA 2018**; and
- (in respect of special category data) in the **public interest**.

(ii) Article 89(1) GDPR

Article 89(1) of the GDPR states that processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, must be subject to 'appropriate safeguards' for the rights and freedoms of the data subject.

The safeguards specified under Article 89(1) GDPR include:

- putting in place technical and organisational measures to protect the rights and freedoms of data subjects, including measures to ensure **data minimisation e.g. pseudonymised personal data**; and
- where the purposes of the research can be fulfilled by using anonymised data, then **anonymised data** should be used.

In the UK, the requirements of Article 89(1) GDPR will not be met unless the provisions of Section 19 DPA 2018 are also complied with.

(iii) Section 19 DPA 2018

Section 19 DPA specifies that the processing must not:

- cause **substantial damage or distress** to individuals; or
- support **measures or decisions with respect to a particular individual**, *unless* the purposes for which the processing is necessary include the purposes of 'approved medical research'.

The term 'approved medical research' has a specific definition in the DPA 2018 which includes medical research carried out by a person who has approval to carry out that research from—

- a research ethics committee recognised or established by the Health Research Authority;
- a relevant NHS body e.g. an NHS trust or NHS foundation trust; or
- United Kingdom Research and Innovation or a body that is a Research Council for the purposes of the Science and Technology Act 1965.

Approved medical research falls under the UK Policy Framework Health and Social Care Research and more information can be found here. If you think that your research falls within the definition of 'approved medical research', this should be highlighted when you are applying for data protection registration and ethical approval through UCL. The steps for these procedures can be found here.

(iv) Exemptions from certain data protection law obligations

The GDPR and the DPA 2018 provide for several exemptions from the rights of data subjects where personal data is processed in a research context, provided the requirements of Article 89(1) and section 19 DPA 2018 are fulfilled.

Where appropriate safeguards are in place, researchers may benefit from exemptions to the following GDPR provisions relating to data subject rights:

- Article 15(1) to (3) GDPR (confirmation of processing, access to data and safeguards for third country transfers);
- Article 16 GDPR (right to rectification);
- Article 18(1) GDPR (restriction of processing);

- Article 21(1) GDPR (objections to processing).

Please note that these exemptions can only be relied upon to the extent that the application of the above GDPR provisions would seriously impair the achievement of your specific research purposes.

You must contact the data protection team immediately if you receive any requests from data subjects wishing to exercise their rights.

E. Summary of appropriate safeguards to be implemented by UCL researchers

Taking into account the legislative provisions set out above, UCL researchers must implement the following 'appropriate safeguards' when carrying out research, in particular research involving the processing of special category information or personal data relating to criminal convictions or offences:

Appropriate Safeguard	**Further Description**
Collect only the minimum amount of personal data required to carry out the research.	You should collect only the personal data required to carry out the research – do not collect any additional personal data simply on the basis that it may be useful in the future. You should also take care to recruit only the number of participants that is necessary for you to fulfil the purposes of the research. You should avoid collecting more personal data than is necessary.
Use pseudonymised personal data.	Where compatible with your research purposes, you should ensure that you use pseudonymised personal data. Please note that where UCL pseudonymises data and holds the key, it will still be classed as personal data for the purposes of data protection legislation. For an overview of the differences between anonymised data and pseudonymised personal data, read this guidance: - Anonymisation and pseudonymisation
Anonymise data where possible.	Personal data should not be used where the research purpose can be fulfilled by further processing with pseudonymised or, better still, anonymised data. See the following for steps to anonymising data: o For quantitative data o For qualitative data, such as removing signatures and names, including a free text anonymisation helper tool from the UK Data Archive o Consider the risks and apply the motivated intruder test o Re-assess any remaining disclosure risk (with guidance from your Risk Management Champion where necessary)

	○ Give consideration to disclosure control For more detailed guidance on anonymization, read the Information Commissioner's code.
Implement safeguards against accidental disclosure and loss or corruption of research data.	You will need to consider carefully technical issues such as how and where the personal data will be stored. It may be appropriate to use the UCL Data Safe Haven service, which provides a technical solution for storing, handling and analysing identifiable data. The Data Safe Haven network also includes tools that can render personal data into anonymous data or pseudonymous personal data. If you choose to operate outside of the Data Safe Haven, any personal data stored on removable media must be strongly encrypted. You will also need to consider how your project is organised and run so that individuals working with personal data are aware of their obligations and treat personal data confidentially and securely. You will also need to assess the information risks associated with your project and any transfers of data. You will need to plan and implement good practice in data management and document this as part of your research process. The plan and execution should form a critical part of the research process. You should ensure that the master copy of your research data is kept secure and on UCL drives or shares. Guidance on how to do all of this is available here: Research Data Policy - Understand your obligations: the policy Information Services Division Guidance - Information Governance services Data Management Plan (DMP) - Introducing a DMP - Writing your DMP - Reviewing your DMP Use the Information classification tool Physical security - It is recommended that researchers consider their physical location when working with personal data

	and do not conduct work where there is a chance of unauthorised persons shoulder-surfing or being able to access any devices used. - Use privacy screens Technical security - Encryption FAQ - How to encrypt your devices using full-disk-encryption: • Windows • Mac OSX • Linux - How to encrypt email and attachments - How to install anti-virus software - How to encrypt your documents Storage - Storage of sensitive data on portable devices and media - Storage of research data - Long term storage of research data - Security of cloud storage and risk assessment Sharing and transfers - Sharing data appropriately - Disclosure control - Information risk tool for transfers Retention and disposal - Data Management Plans - UCL's records retention schedule - Disposal
Ensure that the processing will not cause substantial damage or distress to individuals.	You must ensure that the processing will not cause substantial physical or psychological harm or financial loss to the relevant individuals.
Ensure that the processing will not be used to support measures or decisions with respect to a particular individual.	The only exception to this is where you are carrying out approved medical research (as defined in the DPA 2018).
Comply with relevant UCL policies and procedures and obtain ethics committee approval where required.	You will need to comply with all relevant UCL policies and procedures, including the IT security policy and the data protection policy. You must complete the following training:

	- data protection - information security You must also obtain data protection approval and ethics committee approval for your research project where this is required. UCL policies regarding research data, information security and data protection can be found here: Research Data Policy sets out UCL's expectations around the management data created by UCL researchers. All UCL researchers, supervisors and Principal Investigators should read the Policy and share it with colleagues and students where relevant. Data Protection Policy forms part of UCL's commitment to the safeguarding of personal data processed by its staff and students. Information Security Policy sets out to ensure that UCL computing systems, and all the information held on them, are adequately protected against loss and misuse, and that protection is provided in a cost-effective way. The policy applies to staff and students alike, and to anyone else who has been authorized to use UCL facilities. Research Integrity website provides a list of all UCL policies, statements and code of conduct related to research, including on issues such as ethics or research collaboration. SLMS Research Information Governance Policy (for SLMS staff only) sets out the UCL School of Life and Medical Science's expectations for suitable handling of confidential research information, both personal data and confidential non-personal information.
Comply with relevant ethical standards.	You will need to comply with all applicable ethical standards when carrying out your research; this may include obtaining informed consent of individual participants - see section **E Consent and ethical issues** here for further information on consent – and specialist ethical codes of conduct.
Ensure that special category data is processed in the public interest.	UCL's view is that the data protection and ethics approval processes will help to ensure that research carried out is in the public interest. You should think about how your research is intended to benefit the public when designing the project and applying for the relevant approvals. Please contact us

	using the details set out below if you require further guidance on this point.

F. Third party governance requirements

Please note that specific guidance on appropriate safeguards has been produced by bodies such as the Medical Research Council (see here) and the Health Research Agency (see here). If your research is subject to the governance requirements of any third party such as the HRA or MRC, then you will need to comply with both this UCL guidance note and all relevant requirements imposed by that third party.

G. What to do if there is a security breach of personal data

If there is a security incident involving personal data, you must report it immediately. Follow this guidance.

H. Further guidance

We hope that you find this guidance helpful. If you require any further information on the issues raised in this document, please use the following contact details:

- for **data protection enquiries**, please contact the data protection team at data-protection@ucl.ac.uk; or
- for **ethics enquiries**, please contact the ethics team at ethics@ucl.ac.uk.
- for **information governance queries**, please contact ISD Information Governance services slms.pid@ucl.ac.uk