# Guidance for Supervisors on Data Protection where Students are Processing Personal Data

## A. Introduction

Where students at UCL process personal data as part of their studies (whether they are undergraduates or post-graduates), UCL will be the controller of that personal data. UCL therefore has obligations in respect of that data under data protection legislation, i.e. the General Data Protection Regulation (**GDPR**) and the Data Protection Act 2018 (**DPA 2018**).

Supervisors play an important role in helping UCL to fulfil its legal obligations in relation to the personal data processed by their students, and this guidance note sets out the key points that supervisors should consider in this context. It is designed to be read in conjunction with UCL's other guidance notes for staff on data protection, available here, in addition to existing UCL policies and procedures in relation to data protection in a research context.

This document was last updated on 20 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. Scope

This guidance applies only where UCL staff are supervising students who are processing *personal data*, i.e. information relating to an identified or identifiable living person. If the students are processing *anonymised* data, then this activity falls outside the scope of these guidelines.

## C. What steps must supervisors take to help ensure that students are processing personal data in compliance with data protection legislation?

We have set out a list of steps that supervisors must take where students are processing personal data as part of their studies. Please note that this is not an exhaustive list and that additional measures may be required in certain situations, e.g. if the processing is very high-risk. Please contact the data protection office with any specific queries.

### *(i) Ensure that students are familiar with relevant UCL data protection policies, procedures and guidance*

You must ensure that students are familiar with UCL procedures and guidance on the use of personal data in a research context. In particular:

- all projects involving the use of personal data must be registered with the Data Protection team (see here and here for further information and a link to the registration form);

- you should ensure that your students are familiar with current UCL data protection policies and procedures, including our Data Protection Policy and our IT Security Policy. Key policies are listed here, and outline key technical and other security measures that must be taken in relation to personal data; and

- staff and students must comply with our 'Guidance for researchers on the implications of GDPR and DPA 2018' and our 'Guidance for Researchers on Appropriate Safeguards under the General Data Protection Regulation and the Data Protection Act 2018'. These guidance documents explain key concepts such as:

    - the different types of personal data;

    - the legal basis for processing to be used in a research context;

    - the provision of privacy notices;

    - consent requirements; and

    - the additional safeguards to be put in place where particularly sensitive types of personal data are processed.

### *(ii) Ensure that students complete the appropriate information compliance training*

All staff and students must complete UCL's information compliance training

- Data protection
- Information Security
- Freedom of Information (staff only)

Additional training will also be provided for researchers, and this must be completed once it is available.

### *(iii) Consider data minimisation techniques*

Article 5(1)(c) of the GDPR provides that "*personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').*"

It is therefore important to ensure that students only collect personal data where this is strictly necessary as part of their research.

You should also consider whether it is necessary for students to process fully identifiable data or whether that data may be pseudonymised. Whilst pseudonymised data in respect of which UCL holds the key will still be personal data for the purposes of the GDPR and the DPA 2018, pseudonymisation will help UCL to comply with its obligations in relation to data minimisation. Please see UCL's guidance on anonymisation and pseudonymisation here for further information.

### *(iv) Anonymise data where possible*

Anonymised data, where the data subject is not identifiable, will not fall within the scope of data protection legislation. You should always consider whether students may carry out research using anonymised data rather than personal data.  Please see UCL's guidance on anonymisation and pseudonymisation here for further information.

### *(v) Arrange regular meetings with students*

As their supervisor, you will need to arrange regular meetings with your students to ensure that they are processing personal data in accordance with data protection legislation and UCL policies and procedures. You must discuss their approach to data protection at the beginning of the project and at regular stages after this so that any high-risk processing activities may be identified and dealt with as soon as possible.

## D. 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.