University College London - Appropriate Policy Document

1. About this policy

1.1 This is the "appropriate policy document" for the University College London (**UCL**) setting out how we protect Special Categories of Personal Data and Criminal Convictions Data in accordance with the requirements of Articles 9 and 10 of the UK GDPR and Schedule 1 of the Data Protection Act 2018 (DPA 2018).

1.2 This policy supports UCL's privacy notice documents, including:

(a) General privacy notice - *https://www.ucl.ac.uk/legal-services/privacy/general-privacy-notice*

(b) Staff privacy notice - *https://www.ucl.ac.uk/legal-services/privacy/ucl-staff-privacy-notice*

(c) Student privacy notice - *https://www.ucl.ac.uk/legal-services/privacy/ucl-student-privacy*

1.3 The full list of UCL's privacy notices can be found here: *https://www.ucl.ac.uk/legal-services/privacy*

1.4 This document meets the requirement of the Data Protection Act 2018 that an appropriate policy document be in place where Processing Special Categories of Personal Data and Criminal Convictions Data in certain circumstances.

2. Definitions

(a) **Controller**: the person or organisation that determines when, why and how to Process Personal Data.

(b) **Criminal Convictions and offences Data**: personal data relating to criminal convictions and offences, including Personal Data relating to criminal allegations and proceedings.

(c) **Data Retention Policy**: explains how UCL classifies and manages the retention and disposal of its information. Time periods for retention are set out in the retention schedule (available to view here: *https://www.ucl.ac.uk/library/collections/records-office/retention-schedule*

(d) **Data Subject**: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

(e) **Data Privacy Impact Assessment** (**DPIA**): tools and assessments used to identify and reduce risks of a data processing activity. A DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or organisational change programmes involving the Processing of Personal Data.

(f) **DPA 2018**: the Data Protection Act 2018.

(g) **Data Protection Officer** (**DPO**): the person required to be appointed in specific circumstances under the UK GDPR.

(h) **UK GDPR**: has the meaning as set out in section 3(10) of the DPA 2018, supplemented by section 205(4) of the DPA 2018.

(i) **Personal Data**: any information relating to '…an identified or identifiable natural person ('data subject'); an identifiable natural person 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'. Personal Data includes Special Categories of Personal Data (see below).

(j) **Privacy Notice**: a separate notice setting out information that may be provided to Data Subjects when UCL collects information about them (for staff, this is in the form of the staff privacy notice and for students, this is in the form of the student privacy notice).

(k) **Processing or Process**: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

(l) **Special Categories of Personal Data**: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric data used for the purposes of uniquely identifying someone, or genetic data.

3. Why we process Special Categories of Personal Data and Criminal Convictions Data

3.1 We process Special Categories of Personal Data and Criminal Convictions Data about Data Subjects e.g., our employees, students, research participants and visitors for the purposes listed below. Depending on the context, the data processing activity may involve more than one purpose listed.

Schedule 1, Part 1 Conditions for Processing and Part 2 Substantial Public Interest Conditions:

- **Paragraph 1(1) – Employment, social security and social protection** e.g., assessing an employee's fitness to work; checking applicants' and employees' right to work in the UK;
- **Paragraph 4 – Research etc** e.g., use of medical data including genetic data
- **Paragraph 6(1) – Statutory etc and government** purposes e.g., complying with health and safety obligations;
- **Paragraph 8(1) – Equality of opportunity or treatment** e.g., complying with the Equality Act 2010;
- **Paragraph 9(1) – Racial and ethnic diversity at senior levels of organisations** e.g., conducting analysis of staff levels and racial and ethnic diversity representation across UCL;
- **Paragraph 10(1) – Preventing or detecting unlawful acts** e.g.,
    (i) Responding to requests from third parties e.g., the Police, HMRC and local Councils to support their (criminal) investigations.
    (ii) For disciplinary and investigatory purposes e.g., investigating allegations of sexual misconduct by staff and students.

- **Paragraph 11(1) and 11(2)** – Protecting the public against dishonesty etc e.g., Verifying that employees are suitable for employment or continued employment.

As well as the purposes listed in paragraph 3.1 above, where it is lawful and necessary for us to do so, we may process Special Categories of Personal Data and Criminal Convictions Data about Data Subjects for other purposes as required from time to time. We will make the relevant Data Subject(s) aware of any such other purposes for processing of Special Categories of Personal and Criminal Convictions Data as appropriate.

4. Personal data protection principles

4.1 The UK GDPR requires personal data to be processed in accordance with the six principles set out in Article 5(1). Article 5(2) requires controllers to be able to demonstrate compliance with Article 5(1).

4.2 We comply with the principles relating to Processing of Personal Data set out in the UK GDPR which require Personal Data to be:

(a) Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);

(b) Collected only for specified, explicit and legitimate purposes (Purpose Limitation);

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation);

(d) Accurate and where necessary kept up to date (Accuracy);

(e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation); and

(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).

4.3 We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

5. Compliance with data protection principles

5.1 Lawfulness, fairness and transparency

Personal Data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

We will only Process Personal Data fairly and lawfully and for specified purposes. The UK GDPR restricts our actions regarding Personal Data to specified lawful purposes. We can Process Special Categories of Personal Data and Criminal Convictions Data only if we have a legal ground for Processing and one of the specific Processing conditions relating to Special Categories of Personal Data or Criminal Convictions Data applies. We will identify and document the legal basis and specific Processing condition relied on for each Processing activity within our Record of Processing Activities (**ROPA**). The ROPA is maintained by the Data Protection Team (data-protection@ucl.ac.uk).

When collecting Special Categories of Personal Data and Criminal Convictions Data from Data Subjects, either directly from Data Subjects or indirectly (for example from a third party or publicly available source), we will provide Data Subjects with a Privacy Notice, which sets out all of the

information required by the UK GDPR in a form which is concise, transparent, intelligible, easily accessible and in clear plain language which can be easily understood. All UCL Privacy Notices can be found at: https://www.ucl.ac.uk/legal-services/privacy

5.2 Purpose limitation

Personal Data must be collected only for specified, explicit and legitimate purposes. They must not be further Processed in any manner incompatible with those purposes.

We will only collect personal data for specified purposes and will inform Data Subjects what those purposes are in a published Privacy Notice. We will not use Personal Data for new, different or incompatible purposes from those disclosed when it was first obtained unless we have informed the Data Subject of the new purposes and they have consented where necessary.

5.3 Data minimisation

Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

We will only collect or disclose the minimum Personal Data required for the purpose for which the data is collected or disclosed. We will ensure that we do not collect excessive data and that the Personal Data collected is adequate and relevant for the intended purposes.

5.4 Accuracy

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

We will ensure that the Personal Data we hold and use is accurate, complete, kept up to date and relevant to the purpose for which it is collected by us. We check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. We take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

5.5 Storage limitation

We only keep Personal Data in an identifiable form for as long as is necessary for the purposes for which it was collected, or where we have a legal obligation to do so. Once we no longer need Personal Data it shall be deleted or rendered permanently anonymous.

We maintain a Data Retention Policy and related procedures to ensure Personal Data is deleted after a reasonable time has elapsed for the purposes for which it was being held, unless we are legally required to retain that data for longer.

We will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

5.6 Security, integrity, confidentiality

Personal Data shall be Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

We will implement and maintain reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of or damage to Personal Data.

5.7 Accountability principle

We are responsible for, and able to demonstrate compliance with these principles. Our DPO is responsible for ensuring that we are compliant with these principles. Any questions about this policy should be submitted to the DPO.

We will:

(a) Ensure that records are kept of all Personal Data Processing activities, and that these are provided to the Information Commissioner on request.

(b) Carry out a DPIA for any high-risk Personal Data Processing to understand how Processing may affect Data Subjects and consult the Information Commissioner if appropriate.

(c) Ensure that a DPO is appointed to provide independent advice and monitoring of Personal Data handling, and that the DPO has access to report to the highest management level.

(d) Have internal processes to ensure that Personal Data is only collected, used or handled in a way that is compliant with data protection law.

6. Controller's policies on retention and erasure of personal data

We take the security of Special Categories of Personal Data and Criminal Convictions Data very seriously. We have administrative, physical and technical safeguards in place to protect Personal Data against unlawful or unauthorised Processing, or accidental loss or damage. We will ensure, where Special Categories of Personal Data or Criminal Convictions Data are Processed that:

(a) The Processing is recorded, and the record sets out, where possible, a suitable time period for the safe and permanent erasure of the different categories of data in accordance with our Data Retention Policy.

(b) Where we no longer require Special Categories of Personal Data or Criminal Convictions Data for the purpose for which it was collected, we will delete it or render it permanently anonymous as soon as possible.

(c) Where records are destroyed, we will ensure that they are safely and permanently disposed of.

Data Subjects receive a Privacy Notice setting out how their Personal Data will be handled when we first obtain their Personal Data, and this will include the period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period. The Private Notice is also available on UCL’s website.

7. Review

7.1 This policy on Processing Special Categories of Personal Data and Criminal Convictions Data is reviewed annually.

7.2 The policy will be retained where we process Special Categories of Personal Data and Criminal Convictions Data and for a period of at least six months after we stop carrying out such processing.

7.3 A copy of this policy will be provided to the Information Commissioner on request and free of charge.

Dated: 11 October 2024

Next review: 10 October 2025

Further information:

For further information about our compliance with data protection law, please contact our DPO: data-protection@ucl.ac.uk