LONDON'S GLOBAL UNIVERSITY

UCL Data Protection Policy

Information Security Policy

University College London

Document Summary

Document ID	TBD
Status	Endorsed by the Chair of the Information Risk Governance Group 13-August-2019
Information Classification	Public
Document Version	2.0

University College London, Gower Street, London WC1E 6BT
Tel: +44 (0)20 7679 2000
www.ucl.ac.uk

1 Introduction

1.1 UCL collects, stores and processes the personal data of living individuals such as its staff, students, contractors, research subjects and customers in order to carry out its functions. This processing is regulated by the General Data Protection Regulation 2016 and Data Protection Act 2018 ('data protection law').

1.2 *Personal data* can be defined as any information relating to an identified or identifiable person who can be identified – directly or indirectly – by reference to an identifier such as name, an identification number, location data or online identifier.

2 About this Policy

2.1 The purpose of this policy and the accompanying Data Protection Implementation Guidance is to provide detailed information and advice to ensure compliance with data protection law. The policy covers all UCL activities and processes in which personal data is used, whether in electronic or manual form, and provides a framework for its staff, students and other stakeholders to work within to ensure compliance. The policy forms part of UCL's commitment to the compliant processing of personal data.

3 Scope

3.1 The policy applies to all staff and students when processing personal data on behalf of UCL. 'Staff' includes any individual conducting work at or for UCL and/or its subsidiaries. This includes, but is not limited to, temporary, honorary, visiting, casual, voluntary, emeritus and agency workers, students employed by UCL and its suppliers.

3.2 This policy applies to all personal data processed by UCL in whatever form. This is not restricted by location or method of access.

4 Accountable Roles

4.1 As a controller, UCL has the overall corporate responsibility to comply with data protection law and to be able to demonstrate this.

4.2 The Data Protection Officer (DPO) has primary responsibility for overseeing data protection compliance matters relating to UCL or any of its wholly-owned subsidiaries. This means:

a) Informing and advising UCL of its obligations under data protection law;
b) Monitoring compliance with the regulations and related policies, including raising of awareness and training of staff;
c) Providing procedures, guidance and advice in support of this policy e.g. for Data Protection Impact Assessment (DPIAs);
d) Acting as UCL's first point of contact with the Information Commissioner's Office (ICO);
e) Handling subject access requests and official requests for personal data from third parties; and;
f) Investigating losses and unauthorised disclosures of personal data.

4.3 The responsibilities of Information Asset Owners (IAO) and Information Custodians (IC) are laid out in the Information Management Policy.

4.4 The role of Information Compliance Coordinator is currently being developed.

4.5 Heads of Department / Division are responsible for ensuring their staff understand the data protection principles and for ensuring compliance. They are required to ensure Information

Compliance Officers are designated for their departments and provided with appropriate training and support.

4.6 **All staff** (as defined under the scope of this policy) and students are responsible for:

a) Following this policy and the implementation guidance.
b) Ensuring the processing of personal data (including research data) in all formats is compatible with the data protection principles.
c) Raising any concerns in respect of the processing of personal data with the DPO.
d) Promptly passing on to the DPO any individual requests made under the 'rights of the data subject' as set out in data protection legislation, including subject access requests (SARs) and authorised access requests from third parties for personal data (e.g. Police).
e) Responding promptly to requests from the DPO (or any delegated authority) relating to point (d) above.
f) Reporting data security incidents, losses, near misses or unauthorised disclosures of personal data immediately to the Information Security Group [**isg@ucl.ac.uk**] and cooperating fully and promptly with the incident response team after the incident.
g) Successfully completing UCL's information compliance training, including any refresher training.
h) Registering all research projects that process personal data with the Data Protection Office before processing begins.
i) Completing DPIAs where necessary.
j) Where staff are sharing and processing personal data with other organisations they must ensure appropriate data sharing and processing agreements are in place.

4.7 **Students** process personal data in several ways in the course of their study, such as carrying out research and communicating with staff and fellow students. UCL is the controller of personal data when it is processed as part of a student's programme of studies while at UCL.

a) All postgraduate research students' projects involving processing personal data must be registered with the Data Protection Office before processing begins.
b) All students shall successfully complete the required information compliance training before processing personal data for the purposes of their study.

5 Policy statements

PS1 UCL is committed to complying with the data protection principles. These state that personal data shall be:

(a) Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
(b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; ('purpose limitation');
(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
(d) Accurate and, where necessary, kept up to date; ('accuracy');
(e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; ('storage limitation'); and
(f) 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 ('integrity and confidentiality').

(g) Processed in such a way that UCL shall be responsible for and able to demonstrate compliance with the above six principles ('accountability').

PS2 UCL shall ensure that data protection is incorporated into systems and processes from the outset – referred to as data protection by design and default.

PS3 UCL shall only transfer personal data outside of the European Economic Area where there is adequate protection in place.

PS4 Any incident or 'near miss' that threatens the security of personal data shall be reported to the Information Security Group immediately or as soon as it is known.

PS5 UCL shall adhere to the Privacy and Electronic Communications Regulations (PECR) when engaging in direct marketing activity.

PS6 UCL shall embed Data Protection Impact Assessment (DPIA) completion as a key part of process and activity planning.

PS7 UCL shall uphold the rights of individuals as defined by data protection law.

PS8 The sharing and processing of personal data with other organisations shall be governed by explicit sharing and processing agreements where necessary.

PS9 UCL shall maintain a Record of Processing Activities as required by the Information Commissioner's Office.

PS10 UCL shall respond to all official third-party requests for personal data citing data protection legislation.

PS11 UCL shall ensure that all personal information it owns has a designated Information Asset Owner and Information Custodian at all times. UCL shall ensure timely transfer of these roles whenever necessary (e.g. when staff leave).

PS12 When a member of staff is ceasing employment or a student contract expires they shall not retain any UCL owned personal data unless by an explicit written transfer agreement consistent with the data protection principles.

6 Dependencies

6.1 Documents which rely upon this policy:

- None at present

6.2 Documents which this policy relies on:

- UCL Information Security Policy
- UCL Monitoring Computer and Network Use Policy
- UCL Information Management Policy

7 Related documents

Further useful documents are:

- Data Protection Implementation guidance
- Privacy notices
- DPIA guidance and template
- Data Breach Procedure

8 Stakeholders

The following roles, or their nominated representatives, should be involved in the review of this document

- Policy Owner

- Data Protection Officer
- Head of Information Security
- Chair of Security Working Group

9 Policy owner

This policy is owned by the UCL SIRO.

10 Policy Contact

The Data Protection Officer

11 Review Plan

This document shall be reviewed annually and more frequently if required, e.g. following changes to relevant policies, procedures or legislation.

12 Sanctions

It is a condition of employment that employees abide by the regulations and policies made by UCL. It is a condition of the student contract that students abide by the regulations and policies made by UCL. Any breach of this policy is considered a serious matter and may result in UCL taking disciplinary action.

13 Complaints

Any individual has the right to lodge a complaint about how an organisation is handling personal data. The Information Commissioners Office is the UK's independent body set up to uphold information rights and has published guidance on how to make a complaint.

14 UCL's Governance Framework

This policy is issued under the UCL Information Risk Governance framework under authority delegated from the Senior Management Team.

15 History

Date	Version	Author	Comments
06.08.2019	0.1	Jo McIntosh and Lee Shailer	Apply standard template and layout
30.07.2019	0.2	Reviewed by SWG	
02.08.2019	0.3	John Pelan, Ravi Miranda	Suggestions incorporated via email
06.08.2019	0.4	Paul Lamb, Ravi Miranda	Edited for clarity, template
08.08.2019	0.5	Paul Lamb	Tidy up.

16 Approvals

Endorsed by the Chair of the Security Working Group	8th August 2019
Endorsed by the Chair of the Information Risk Management Group	11th August 2019
Endorsed by the Chair of the Information Risk Governance Group	13th August 2019

Appendix A: Definitions

UCL has adopted the EU GDPR definitions, which include:

i) Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

ii) Controller – the natural or legal person, public authority or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data

iii) Processor – a natural or legal person, public authority agency or other body which processes personal data on behalf of the controller

iv) Personal data breach – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed

v) Special category personal data – personal data which is more sensitive and needs greater protection. For example, information about an individual's
   a. Race or ethnic origin
   b. Politics
   c. Religion
   d. Trade union membership
   e. Genetics
   f. Biometrics
   g. Health
   h. Sex life and sexual orientation

   Personal data relating to criminal offences/convictions are not included, but similar extra safeguards apply to its processing

The full list of definitions is available at http://www.privacy-regulation.eu/en/article-4-definitions-GDPR.htm