LONDON'S GLOBAL UNIVERSITY

UCL Data Protection Policy

Information Security Policy

University College London

Document Summary

Document ID	TBD
Status	Approved
Information Classification	Public
Document Version	Approved by the Information Risk Governance Group 10 April 2017

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

1. Purpose and objectives

This policy forms part of University College London's commitment to the safeguarding of personal data processed by its staff and students. (Processing has a very broad definition, and includes activities such as creating, storing, consulting, amending, disclosing and destroying data.) Its objectives are:

- To help staff and students recognise personal data
- To help them understand their rights and obligations with respect to personal data for which UCL is data controller or has been designated as data processor.

2. Introduction

UCL processes the personal data of living individuals such as its staff, students, contractors, research subjects and customers. This processing is regulated by the Data Protection Act 1998 (DPA). The UK's regulator for the DPA is the Information Commissioner's Office.

It is the duty of data controllers such as UCL to comply with the data protection principles (see the Annex to this Policy) with respect to personal data. This policy describes how UCL will discharge its duties in order to ensure continuing compliance with the DPA in general and the data protection principles and rights of data subjects in particular. The principles are listed in the Annex to this Policy.

3. Scope

This policy is a supporting policy of the UCL Information Security Policy. Its scope is as defined in section 1.4 of that Policy:

"The policy applies to all staff and students of UCL and all other computer, network or information users authorized by the College or any department thereof. It relates to their use of any UCL-owned facilities (and those leased by or rented or on loan to UCL), centrally managed or otherwise; to all private systems (whether owned, leased, rented or on loan) when connected to the UCL network; to all UCL-owned or licensed data and programs (wherever stored); and to all data and programs provided to UCL by sponsors or external agencies (wherever stored). The policy also relates to paper files and records created for the purposes of UCL business."

4. Roles and responsibilities

Information Risk Governance Group (IRGG)

The IRGG is a standing committee accountable to the Risk Management Working Group (RMWG). Its purpose is to support and drive the effective management of information risk across UCL, and to provide the RMWG with the assurance that best practice mechanisms for information governance are in place across UCL.

Information Risk Management Group (IRMG)

The IRMG is a standing committee accountable to the IRGG. Its purpose is to monitor, assess and prioritise information risks, and forward risk treatment proposals to the IRGG for review. The IRMG's secondary role is to consult with the broader community of Deans and Heads of Faculty to validate risk treatment proposals, and identify how to transcend any cultural, economic or organisational barriers to implementation.

The IRMG will operate in concert with its peer group, the Security Working Group (SWG) to ensure that both the technical and business aspects of information risk are taken into account in risk treatment activities.

The scope of the IRMG includes information in all its forms and includes, for example, paper-based information as well as information held electronically.

Security Working Group (SWG)

The SWG is a standing committee accountable to the Infrastructure & Common IT Shared Services Group (IISG). Its purpose is to classify any identified concerns as "new and real risks" or as "no concern". The SWG will advise on threats and vulnerabilities, identify and highlight shared UCL issues, and create ad hoc groups to facilitate the development of risk treatment proposals.

The SWG will operate in concert with its peer group, the IRMG to ensure that both the technical and business aspects of information risk are taken into account in risk treatment activities.

Data Protection Officer

The Data Protection Officer has primary responsibility for UCL's compliance with the DPA. This comprises:

- maintaining UCL's notification with the Information Commissioner's Office
- ensuring completion of the Annual Survey of Personal Data Holdings
- handling subject access requests and requests from third parties for personal data
- promoting and maintaining awareness of the DPA and regulations, including training
- investigating losses and unauthorised disclosures of personal data.

The DPO is UCL's main contact for the Information Commissioner's Office.

Heads of Department / Division

Heads of Department / Division are responsible for ensuring their staff understand the role of the data protection principles in their day-to-day work, through induction, training and performance monitoring, and for monitoring compliance within their own areas of responsibility. They should also ensure Data Protection Coordinators are designated for their departments or divisions, and provided with appropriate training and support.

Data Protection Coordinators

Coordinators are required to:

- advise staff and students in their departments on the implementation of and compliance with this policy and any associated guidance / codes of practice
- ensure appropriate technical and organisational measures are taken within their departments to ensure against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
- support UCL's notification with the Information Commissioner's Office by maintaining the register of holdings of personal data, including databases and relevant filing systems, and the purposes of processing
- keep the Data Protection Officer informed of changes in the collection, use, and security of personal data within their department
- report any loss of personal data to the Head of Department / Division and the Data Protection Officer
- ensure the proper completion of applications for the data protection registration of new research projects before they are submitted to the Records Office
- confirm compliance with the PCI Data Security Standard in relation to the records of credit card payments made through the department.

Data Owner

Data Owners are responsible for:

- establishing and monitoring measures, in accordance with this policy and the information security policy, to protect any holdings of personal data for which they are responsible
- ensuring that those holdings are registered as part of the annual survey of personal data holdings

- ensuring that any transfer of personal data to third parties is authorised, lawful and uses appropriate safe transport mechanisms such as encryption.
- authorising the downloading of electronic personal data on to portable devices or the removal of manual personal data from UCL premises
- informing their departmental Data Protection Coordinator when new holdings of personal data are established or when the purposes of processing change.

Data Custodians

Data Custodians should ensure that their processing of personal data is compatible with the data protection principles, including the security and integrity of data sets.

Data Processors

Data processors have a contractual responsibility to act only on UCL's instructions and to ensure that their processing of personal data provided by UCL is carried out in compliance with this policy and in accordance with the eight data protection principles. There should be a written agreement with data processors which adequately addresses these responsibilities.

Staff and students

All staff and students are responsible for:

- ensuring that their processing of personal data, including research data, in all formats (e.g. electronic, microfiche, paper, etc.) is compatible with the data protection principles
- raising any concerns in respect of the processing of personal data with the Data Protection Officer
- promptly passing on to the Data Protection Officer all subject access requests and requests from third parties for personal data
- reporting losses or unauthorised disclosures of personal data to the Data Protection Coordinator.

In order that UCL can continue to comply with the fourth data protection principle, staff and students should ensure the personal data they provide about themselves is up to date.

5. Security of personal data

All staff and students processing personal data for which UCL is data controller or has been designated as data processor should ensure that the data are secure: appropriate measures must be taken to prevent unauthorised access, disclosure and loss. Staff

whose work includes responsibility for supervision of students have a duty to ensure that students observe the eight principles of the Act.

It should not be necessary to store electronic personal data on portable devices such as laptops, USB flash drives, portable hard drives, CDs, DVDs, or any computer not owned by UCL. Similarly, personal data should not be regularly removed from UCL premises. In the case of electronic data, to minimise the risk of loss or disclosure, a secure remote connection to UCL must be used.

Use of externally hosted services (e.g. cloud) for the processing of personal data for which UCL is the data controller or has been designated as a data processor should be restricted to services for which UCL has entered into an enterprise agreement. Assurance must also have been provided by the vendor that personal data will not be transferred outside the EEA without an adequate level of protection. Advice and approval should be sought from the Data Protection Officer before entering into an agreement with a vendor based outside the EEA.

Downloading personal data on to portable devices or taking personal data off-site must be authorised in writing by the Data Owner, who must explain and justify the operational need in relation to the volume and sensitivity of the data. The data must be strongly encrypted. Users should only store the data necessary for their immediate needs and should remove the data as soon as possible. To avoid loss of encrypted data, or in case of failure of the encryption software, an unencrypted copy of the data must be held in a secure environment. The Information Security Group's guidance on encryption should be followed:
https://www.ucl.ac.uk/informationsecurity/itsecurity/knowledgebase/securitybaselines/encryption

Manual personal data and portable electronic devices should be stored in locked units, and they should not be left on desks overnight or in view of third parties.

In order to comply with the fifth data protection principle personal data should be securely destroyed when no longer required, with consideration for the format of the data. The Information Security Group's guidance should be followed for electronic data:
https://www.ucl.ac.uk/informationsecurity/itsecurity/knowledgebase/securitybaselines/secure_disposal_guidelines

Personal data must not be disclosed unlawfully to any third party. Transfers of personal data to third parties must be authorised in writing by the data owner and protected by adequate contractual provisions or data processor agreements, agree with UCL's notification and must use safe transport mechanisms.

All losses of personal data must be reported to the Departmental Data Protection Coordinator and the Data Protection Officer. Negligent loss or unauthorised disclosure

of personal data, or failure to report such events, may be treated as a disciplinary matter and could be considered gross misconduct.

6. Publication of staff information

UCL will make public as much corporate information as possible. The following types of personal information will usually be published:

- Names of members of the Council and the Provost's Senior Management Team
- Directories of staff, including name, internal telephone number and UCL email address
- Research expertise and academic achievements of academic and research staff
- Publication of research grants and awards

However, there are circumstances in which, for security and other reasons, agreed subsets of the above data about UCL staff will not be published in line with UCL's ex-directory policy. See ***http://www.ucl.ac.uk/isd/how-to/ucl-directory/ucl-directory-ex-directory*** for further information.

7. Access to personal data

7.1. Subject access rights

Data subjects have a right of access to their personal data, including some unstructured manual personal data. Subject access requests must be made in writing, including Form 6 (***https://www.ucl.ac.uk/legal-services/dp-subject-access-request***) or otherwise and sent to the Data Protection team. Data subjects must prove their identity.

Copies will be provided in permanent form promptly and in any event within 40 days. In the case of a request made in relation to examination marks or results, the timescale is extended to the earlier of:

- five months from the day on which the request was received; or
- 40 days from the announcement of the examination results.

Some personal data are exempt from the right of subject access, including confidential references provided by UCL, examination scripts and some research data.

UCL does not charge a fee for subject access requests.

7.2. Monitoring

It is sometimes necessary for UCL to monitor information and communications. This may include personal data. The circumstances in which monitoring may be carried out, and procedures for doing so, are described in the UCL Policy on Monitoring

Computer and Network Use:
https://www.ucl.ac.uk/informationsecurity/policy/policy/public-policy/Monitoring

7.3. Third party access

In certain circumstances the DPA provides for disclosure of personal data, without the consent of the data subject, to certain organisations. Requests for such disclosures from third parties, such as the police, UK Border Agency, local authorities or sponsors, should be made in writing and handled by the Data Protection Officer. This will ensure the validity of the request and any warrants or orders of court can be checked. Staff disclosing personal data may not be protected by an invalid warrant.

8. Records Management

Records in all formats containing personal data must be created, stored and disposed of in accordance with UCL's Records Management Policy and any associated procedures and codes of practice. They must be authentic, reliable and usable and capable of speedy and efficient retrieval. They must be retained for no longer than the periods permitted in UCL's retention schedule and, when no longer required for operational reasons, must be transferred to UCL's in-house records storage facility or institutional archive (if selected for permanent preservation) or disposed of securely and confidentially.

UCL Records Management Policy is here: ***http://www.ucl.ac.uk/library/about/records-office/policy***

UCL Retention Schedule is here: ***http://www.ucl.ac.uk/library/about/records-office/retention***

9. Research using personal data

Personal data processed for research, statistical and historical purposes must not be used to support decisions with respect to data subjects or processed so as to cause them substantial damage or distress. Notwithstanding the fifth data protection principle, such data may be kept indefinitely. They may also be further processed for other research purposes and are exempt from the right of subject access as long as the results of the research do not identify data subjects.

Staff and students using personal data for which UCL is data controller or has been designated as data processor in research must:

- understand how personal data may be used in research
- use the minimum data necessary for the research, including, wherever possible, anonymised or pseudonymised data
- ensure their processing complies with all the data protection principles

- inform Data Protection Coordinators about research before processing of personal data begins
- register all research projects involving personal data with the Data Protection team before processing begins
- where relevant, inform data subjects about the purposes of the processing and ensure valid written consent is obtained
- ensure all personal data collected are necessary for the purpose(s) of the research
- keep the data securely
- ensure personal data are destroyed confidentially, stored with the Records Office or otherwise disposed of in compliance with agreements with funders.

10. Status

This document is a part of UCL's information security policy and has been approved by UCL's Information Strategy Committee. It is a condition of employment that employees will abide by the regulations and policies made by UCL. Likewise, these latter are an integral part of the regulations for students.

ANNEX

THE DATA PROTECTION PRINCIPLES

It is the duty of data controllers and data processors to comply with all the data protection principles. These are set out in Schedule 1 of the Data Protection Act 1998, from which the following extract is taken:

1) Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-
   a) at least one of the conditions in Schedule 2 is met, and
   b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2) Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3) Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4) Personal data shall be accurate and, where necessary, kept up to date.
5) Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6) Personal data shall be processed in accordance with the rights of data subjects under this Act.
7) Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8) Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Document Control Sheet

Revision History

Date of this revision: 10.01.2017

Date of next revision: TBD

Revision date	Summary of Changes
10.01.2017	**Section 1 Purpose and Objectives** added "*for which UCL is data controller or has been designated as data processor" to "To help them understand their rights and obligations with respect to personal data*"
	Section 4 Roles and responsibilities ***Deleted*** *"Information Strategy Committee* *The Committee is responsible for defining UCL's information security policy and for ensuring it is discharged by all academic and administrative departments and divisions through Heads of Departments."* ***Added*** *"Information Risk Governance Group (IRGG)* *The IRGG is a standing committee accountable to the Risk Management Working Group (RMWG). Its purpose is to support and drive the effective management of information risk across UCL, and to provide the RMWG with the assurance that best practice mechanisms for information governance are in place across UCL."* ***Deleted*** "*ICT Infrastructure Sub-Committee* *ICT Infrastructure Sub-Committee advises the ISC on matters related to compliance with this policy, and is responsible for regularly reviewing it for completeness, effectiveness and usability."* ***Added*** "*Information Risk Management Group (IRMG)* *The IRMG is a standing committee accountable to the IRGG. Its purpose is to monitor, assess and prioritise information risks, and forward risk treatment proposals to the IRGG for review. The IRMG's secondary role is to consult with the broader community of Deans and Heads of Faculty to validate risk treatment proposals, and identify how to transcend any cultural, economic or organisational barriers to implementation.* *The IRMG will operate in concert with its peer group, the Security Working Group (SWG) to ensure that both the technical and business aspects of information risk are taken into account in risk treatment activities.* *The scope of the IRMG includes information in all its forms and includes, for example, paper-based information as well as information held electronically."* ***Deleted*** *"The Security Working Group acts as a focus for technical and other issues relating to information security and data protection within UCL. It makes recommendations to the ICTISC on strategy and policy matters in relation to data protection, and receives reports from the Data Protection Officer."*

	Added *"The SWG is a standing committee accountable to the Infrastructure & Common IT Shared Services Group (IISG). Its purpose is to classify any identified concerns as "new and real risks" or as "no concern". The SWG will advise on threats and vulnerabilities, identify and highlight shared UCL issues, and create ad hoc groups to facilitate the development of risk treatment proposals.* *The SWG will operate in concert with its peer group, the IRMG to ensure that both the technical and business aspects of information risk are taken into account in risk treatment activities."* ***Deleted*** *"(data-protection@ucl.ac.uk)"*
	5 Security of personal data ***Inserted*** *"for which UCL is data controller or has been designated as data processor"* ***Replaced*** *"is rarely"* ***with*** *"should not be"* ***Deleted*** *"manual"* ***Replaced*** *"should"* ***with*** *"must"* ***Deleted*** *"wherever possible"* ***Added*** *"Use of externally hosted services (e.g. cloud) for the processing of personal data for which UCL is the data controller or has been designated as a data processor should be restricted to services for which UCL has entered into an enterprise agreement. Assurance must also have been provided by the vendor that personal data will not be transferred outside the EEA without an adequate level of protection. Advice and approval should be sought from the Data Protection Officer before entering into an agreement with a vendor based outside the EEA."* ***Deleted*** *"manual"* ***Replaced*** *"Computer Security Team's"* ***with*** *"Information Security Group's"* ***Updated URL*** *"https://www.ucl.ac.uk/informationsecurity/itsecurity/knowledgebase/securitybaselines/encryption"* ***Updated URL*** *"https://www.ucl.ac.uk/informationsecurity/itsecurity/knowledgebase/securitybaselines/secure_disposal_guidelines"*
	6 Publication of staff information ***Deleted*** *"Lists and"* ***Deleted*** *"However, there are circumstances in which, for security and other reasons, agreed subsets of the above data about UCL staff will not be published. This is not within the scope of the Data Protection Act but is subject to UCL's ex-directory policy."*

	Added *"However, there are circumstances in which, for security and other reasons, agreed subsets of the above data about UCL staff will not be published in line with UCL's ex-directory policy.* ***See http://www.ucl.ac.uk/isd/how-to/ucl-directory/ucl-directory-ex-directory*** *for further information***"**
	7.1. Subject access rights ***Updated URL*** *https://www.ucl.ac.uk/legal-services/dp-subject-access-request* ***Replaced*** *"Officer"* ***with*** *"team"* ***Inserted word*** *"some"* ***in the line*** "examination scripts and <u>some</u> research data" ***Deleted*** *"Although the DPA applies only to living individuals, data about deceased persons who at the time of processing would be under 100 years old should be treated as personal data, unless the information is the subject of a valid request under Freedom of Information legislation."* ***7.2. Monitoring*** ***Updated URL*** *https://www.ucl.ac.uk/informationsecurity/policy/policy/public-policy/Monitoring*
	8. Records Management ***Added URLs:*** *"UCL Records Management Policy is here: http://www.ucl.ac.uk/library/about/records-office/policy* *UCL Retention Schedule is here: http://www.ucl.ac.uk/library/about/records-office/retention"*
	9. Research using personal data ***Inserted text*** *"for which UCL is data controller or has been designated as data processor"* **in line** "*Staff and students using personal data <u>for which UCL is data controller or has been designated as data processor</u> in research must:"* ***Replaced*** *"Records Office"* ***with*** *"Data Protection team"*
	Section 4 - Definitions from the earlier document have been moved to the common Glossary, this has resulted in subsequent sections being renumbered

Approvals

Approved by the Chair of the Information Strategy Committee	**15-Feb-2011**
Endorsed by the Security Working Group	**22-Feb-2017**
Endorsed by the Information Risk Management Group	**30-Mar-2017**
Approved by the Information Risk Governance Group	**10-Apr-2017**