LONDON'S GLOBAL UNIVERSITY

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 6-Sep-2016

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

1. Introduction

1.1. As a centre of knowledge and training, University College London focuses on exploiting information. Next to people, information is UCL's most important asset. The information we use exists in many forms: printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Regardless of the form it takes, or means by which it is shared or stored, information should always be protected appropriately.

1.2. Information security is characterized here as being concerned with guaranteeing availability (ensuring that authorized users always have access to information when they need it), integrity (safeguarding its accuracy and completeness), confidentiality (ensuring that sensitive information is accessible only to those authorized to use it), and authenticity. It must also address proper methods of disposal of information that is no longer required. Security is essential to the success of almost every academic and administrative activity. Effective security is achieved by working within a proper framework, in compliance with legislation and UCL policies, and by adherence to approved procedures and codes of practice.

1.3. The objectives of this information security policy are to:

- ensure that all of UCL's computing facilities, programs, data, network and equipment are adequately protected against loss, misuse or abuse, and that this protection is cost-effective;
- ensure that all users are aware of and fully comply with this policy statement and all associated policies, and are aware of and work in accordance with the relevant procedures and codes of practice;
- ensure that paper records are kept securely and managed effectively;
- ensure that all users are aware of and fully comply with the relevant UK and European Union legislation;
- create across UCL an awareness that appropriate security measures must be implemented as part of the effective operation and support of information management systems;
- ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data they handle;
- ensure that information is disposed off in an appropriately secure manner when it is no longer relevant or required.

1.4. The policy applies to all staff and students of UCL and all other computer, network or information users authorized by UCL or any department or division 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.

1.5. Definitions of the terms used in this policy statement and supporting documentation may be found in the glossary at **http://www.ucl.ac.uk/isd/common/cst/swg/policy/public-policy/Glossary.**

1.6. The UCL Senior Management Team has approved this policy statement and delegated its implementation to Heads of Departments and Divisions.

1.7. Those requiring information, explanation or training about any aspects of the policy which relate to computer security should discuss their needs with the UCL Information Security Group. Questions about the creation, classification, retention and disposal of records (in all formats) should be taken to the Records Manager. The UCL Information Security Group and the Data Protection Officer will in the first instance be responsible for interpretation and clarification of the information security policy.

2. Responsibilities for Information Security

2.1. All who make use of UCL's systems and information have responsibility for protecting those assets. Individuals must, at all times, act in a responsible and professional way in this respect, and will refrain from any activity that may jeopardize security.

2.2. The Information Risk Governance Group (IRGG) is responsible for defining an information security policy and for ensuring it is discharged by all academic and administrative departments and divisions through the respective Head of Department. The policy will normally apply to associated bodies, including UCL-owned companies.

2.3. Heads of Department and Divisions are required to implement this policy in respect of both paper and electronic systems operated by their Departments or Divisions and are responsible for ensuring that staff, students and other persons authorized to use those systems are aware of and comply with it and associated codes of practice. They are required to appoint a Custodian for each system operated by them, and a departmental network administrator, whose duties and training requirements are set out in codes of practice associated with the information security policy. Heads of Department should ensure adequate oversight of security (in consultation with the UCL Information Security Group), through departmental computing support staff or otherwise. The roles of Custodians and departmental

network administrators may be shared across smaller departments whenever appropriate, but the Head of Department remains responsible for ensuring the roles are fulfilled.

2.4. Operational responsibility for records management is delegated to the Records Manager, who is responsible for the development of procedures, advice on good practice and promotion of compliance with the UCL Records Management Policy (**http://www.ucl.ac.uk/library/about/records-office/policy**), which applies to all records in any format.

2.5. The IRGG advises the UCL Risk Management Working Group on matters related to compliance with this policy, and is responsible for regularly reviewing it for completeness, effectiveness and usability. The Information Risk Management Group (IRMG), in collaboration with the Security Working Group and the UCL Information Security Group, will from time to time make available supplementary procedures and codes of practice, and promote them throughout UCL; once approved by the IRGG these will also become UCL policy and will be binding on departments.

The IRMG will also arrange for analysis of security assessments received from departments and divisions, and report on these to the IRGG.

2.6. The UCL Information Security Group, in addition to its involvement in policymaking, provides relevant operational services. These include incident response and co-ordination, dissemination of security information, training, consultancy, and liaison with other external security teams and law enforcement agencies.

2.7. It is the responsibility of each individual to ensure his/her understanding of and compliance with this policy and any associated procedures or codes of practice.

2.8. Staff with supervisory responsibility should make their supervised staff or students aware of best practice.

2.9. Staff and students who process or who are responsible for the processing of personal data, as defined in UCL's Data Protection Policy, are additionally required to understand and comply with all obligations placed upon them under agreements with external parties, including but not limited to information security, integrity and perpetual confidentiality.

3. Compliance with Legislation

3.1. UCL, each member of staff, and its students have an obligation to abide by all UK legislation and the relevant legislation of the European Union. Of particular importance in this respect are the Computer Misuse Act 1990, the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000, the Terrorism Act 2006 and the Counter Terrorism and Security Act 2015.

This policy satisfies the Data Protection Act's requirement for a formal statement of UCL's security arrangements for personal data. The requirement for compliance devolves to all users defined in (1.4) above, who may be held personally responsible for any breach of the legislation.

3.2. Relevant legislation is referenced in supporting polices and guidelines. Full texts are available from The Stationery Office and at **http://www.legislation.gov.uk/ukpga/1998/29/contents**

4. Risk Assessment and Security Review by Departments/Divisions

4.1. Information should be suitably classified according to the guidance given in "Classification of information held by UCL personnel, for security management purposes". **https://www.ucl.ac.uk/informationsecurity/policy/internal-policy/Guidelines10**

Custodians should adopt a risk-based approach to assessing the value of information handled, its sensitivity and the appropriateness of security controls in place or planned. Without proper assessment of the value of information assets, and the consequences (financial, reputational and otherwise) of loss of data or disruption to service, efforts to improve security are likely to be poorly targeted and ineffective. Similarly, periodic review is necessary to take into account changes to technology, legislation, business requirements and priorities; security arrangements should be revised accordingly.

4.2. Heads of Department should establish effective contingency plans appropriate to the outcome of any risk assessment. They are also required to re-evaluate periodically the security arrangements for their information management systems - at least once every three years, and additionally in response to significant departmental changes (such as turnover of key staff, commissioning of new systems etc.). A formal report must be submitted to the Information Risk Governance Group via the Information Risk Management Group.

5. Breaches of Security

5.1. Any individual suspecting that the security of a computer system has been, or is likely to be, breached should inform the UCL Information Security Group (ISG) immediately. UCL ISG will advise UCL on what steps should be taken to avoid incidents or minimize their impact, and identify action plans to reduce the likelihood of recurrence.

5.2. In the event of a suspected or actual breach of security, UCL ISG may, after consultation with the relevant Custodian or Head of Department, require that any unsafe systems, user/login names, data and/or programs be removed or made inaccessible.

5.3. Where a breach of security involving either computer or paper records relates to personal information, the UCL Data Protection Office must be informed, as there may be an infringement of the Data Protection Act 1998 which could lead to civil or criminal proceedings. It is vital, therefore, that users of UCL's information systems comply, not only with this policy, but also with UCL's Data Protection Policy and associated codes of practice, details of which may be found on the UCL website.

5.4. All physical security breaches should be reported to UCL Security.

5.5. ISD will monitor network activity, receive reports from the UCL Information Security Group and other security agencies, and take action or make recommendations consistent with maintaining the security of UCL information assets.

5.6. The Provost or his deputy has the authority to take whatever action is deemed necessary to protect UCL against breaches of security.

6. Policy Awareness and Disciplinary Procedure

6.1. The contract of employment shall state that employees are required to comply with the Information Security Regulations, including such additions or amendments thereto as may be made by UCL from time to time.

6.2. As part of the induction process, Managers are reminded via the standard checklist to ensure that the online information security awareness training is completed.

6.3. Students are required to comply with the Information Security Regulations, including such additions or amendments thereto as may be made by UCL from time to time.

6.4. Existing staff and students of UCL, authorized third parties and contractors given access to the UCL network will be advised of the existence of this policy statement and the availability of the associated procedures, codes of practice and guidelines which are published on the UCL website. Failure of an individual student or member of staff to comply with this policy may lead to the instigation of disciplinary procedures and, in certain circumstances, legal action may be taken. Failure of a contractor to comply could lead to the cancellation of a contract.

7. Supporting Policies, Procedures and Codes of Practice

7.1. Supporting policies, procedures and codes of practice amplifying this policy statement are published with it and are available on the UCL website. Staff, students, contractors and other third parties authorized to access the UCL network to use the systems and facilities identified in paragraph (1.4) of this policy, are required to familiarize themselves with these and to work in accordance with them. Guidance notes will also be published to facilitate this.

7.2. The National Health Service places additional obligations on users of NHS service user data. UCL requires compliance with these. Additional related UCL School of Life & Medical Sciences policies, procedures and guidance can be found at **http://www.ucl.ac.uk/slms/ident-data/**

7.3. Personal data (as defined by the Data Protection Act, 1998) must be stored securely; if such data is held on mobile devices (e.g. smartphones) or removable media, it must be strongly encrypted, in compliance with the Data Protection Policy and the Corporate Digital Data Ownership and Access Policy. Other forms of sensitive business data, intellectual property, etc. should, similarly, be strongly encrypted. The Information Security Group will issue and keep under review guidance on what constitutes an acceptable standard of encryption.

7.4. Any outsourced information services must be subject to a documented contract which must comply with the guidelines in "Security considerations in outsourced IT arrangements".

8. Status of the Information Security Policy

8.1. This policy statement does not form part of a formal contract of employment with UCL, but 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.

Document Control Sheet
Revision History

Date of this revision: June 17 2016

Date of next revision: TBD

Revision date	Summary of Changes	Changes marked
17.06.2016	3.2 Updated text 'Her Majesty's Stationery Office' and 'The Stationery Office (TSO)'	Y
	4.1 Added "Information should be suitably classified according to the guidance in UCL Corporate Digital Data Ownership and Access Policy (.doc - public view)"	Y
	4.2 Replaced "Information Services Governance Committee" with "Information Risk Governance Group'	Y
	5.5 Replaced 'ISD Technology Services' with 'IT Services Delivery'	Y
	6.1 Check with HR and SRS	N/A
	6.2 Moved to section 1.7	Y
	7.3 Replaced 'laptops' with 'smartphones'	Y
	7.4 Replaced 'IT Support' with 'outsourced IT Services'	Y
	7.4 Replaced 'written contract' with 'documented contract'	Y
24.06.2016	Removed letterhead	N/A
	1.4 (and elsewhere) Replaced "department" with department or division"	Y
	1.5 Corrected URL	Y
	2.2 Replaced "ISGC" with "IRGG".	Y
	2.4 Updated URL	Y
	2.5 Replaced "ISGC" with "IRGG"; "IISG" with "IRMG".	Y
	3.1 Added "the Terrorism Act 2006 and the Counter Terrorism and Security Act 2015".	Y
	3.2 Updated URL	Y
	4.1 Changed to the Classification Guidelines	Y
	4.2 Replaced "ISGC" with "IRGG".	Y
	5.5 Changed "TS" to "ISD"	Y

	6.1 Updated HR action.	Y
	7.4 Replaced “IT” with “information services”.	Y
26.07.2016	6.1 Added text from Registry covering students	Y
02.08.2016	7.4 Removed “support”	N/A
	6.1 Split section 6.1 into 4 sections for readability. Removed “additionally”	N/A
22.08.2016	Tidied the header; added “for consideration by IRMG…”.	N/A
24.08.2016	Changed header to “Endorsed by the Information Risk Management Group. For consideration by the Information Risk Governance Group.”	N/A
06.09.2016	Changed header to “Approved by the Information Risk Governance Group.”	N/A

Approvals

Approved by the Information Services Governance Committee	**17 July 2013**
Endorsed by the Security Working Group (subject to the change below)	**11-Jul-2016**
SWG chair added text from Registry to #6.1	**26-Jul-2016**
Endorsed by the Information Risk Management Group	**24-Aug-2016**
Approved by the Information Risk Governance Group	**6-Sep-2016**