UNIVERSITY OF LONDON

# Information Security Policy (ISP-001)

## 1 Introduction

1.1 The University recognises that Information is fundamental to its effective operation and, next to staff, is its most important business asset. The purpose of this Information Security Policy is to ensure that the information managed by the University is appropriately secured in order to protect against the possible consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information. Failure to adequately secure information increases the risk of financial and reputational loss to the University.

1.2 This overarching policy document provides management direction and support for information security and lists a set of component sub-policy documents which taken together constitute the Information Security Policy of the University.

## 2 Purpose

The objectives of this policy are to:

2.1 Ensure that all information and information systems within the University are protected to the appropriate level.

2.2 Ensure that all users are aware of and comply with this policy including sub-policies and all current and relevant UK and EU legislation.

2.3 Provide a safe and secure information systems environment for staff, students and any other authorised users.

2.4 Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data that they handle.

2.5 Protect the University from liability or damage through the misuse of information or information systems.

2.6 Ensure that information is disposed of in an appropriately secure manner when it is no longer relevant or required.

## 3 Scope

3.1 The Information Security Policy applies to information in all its forms, collectively termed ‘information assets’ within this document. It covers information in paper form, stored electronically or on other media, information transmitted by post, by electronic means and by oral communication, including telephone and voicemail. It includes text, pictures, audio and video. It applies throughout the lifecycle of the information from creation through storage and utilisation to disposal. Appropriate protection is required for all forms of information to ensure business continuity and to avoid breaches of the law and statutory, regulatory or contractual obligations.

3.2 For the purposes of this document, The University is defined as the central administrative and academic departments of the University of London, including the School of Advanced Study and member institutes, International Programmes, Senate House Libraries, CoSector, Student Central, Intercollegiate Halls of Residence and the University of London Institute in Paris.

3.3 This policy applies to all staff, students and other members of the University and third parties who interact with information held by the University and the information systems used to store and process it, collectively termed ‘users’ throughout this document.

3.4 For the purposes of this document, information security is defined as the preservation of:

- Confidentiality (protecting information from unauthorised access and disclosure)
- Integrity (safeguarding the accuracy and completeness of information)
- Availability (ensuring that information and associated services are available to authorised users when required)

## 4 Information Security Principles

The following principles underpin this policy:

4.1 Information will be protected in line with all relevant University policies and legislation.

4.2 It is the responsibility of all individuals to be mindful of the need for information security across the University and to be aware of and comply with this policy including sub-policies and all current and relevant UK and EU legislation.

4.3 Each information asset will have a nominated owner who will be assigned responsibility for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect the asset.

4.4 All information will be classified according to a level of risk (section 5).

4.5 Information will be made available solely to those who have a legitimate need for access.

4.6 It is the responsibility of all individuals who have been granted access to information to handle it appropriately in accordance with its classification.

4.7 The integrity of information will be maintained.

4.8 Information will be protected against unauthorised access.

## 5 Information Classification

The following table provides a summary of the risk based information classification levels that have been adopted by the University. Further information is provided in the Data Classification Policy.

| Classification Level | Description | Examples |
|---|---|---|
| High | Loss, misuse or unauthorised access to this data could result in significant financial loss, reputational loss and litigation. | Student data<br>Staff data<br>Financial data<br>Graduates and alumni<br>Customers and clients |
| Medium | Loss, misuse or unauthorised access could result in reputational loss and litigation. | Teaching data<br>Research data<br>Estates data<br>Governance records |
| Low | Loss, misuse or unauthorised access could result in reputational loss. | Management information<br>Collections data<br>Public facing content |

## 6 Legal and Regulatory Obligations

The use of information is governed by a number of different Acts of Parliament. All users have an obligation to comply with current relevant legislation which includes, but is not limited to:

- Computer Misuse Act (1990)
- The Data Protection Act (1998)
- Freedom of Information Act (2000)
- Copyright, Designs and Patents Act (1988)
- Regulation of Investigatory Powers Act (2000)
- Human Rights Act (2000)
- Electronic Communications Act (2000)
- Digital Economy Act (2010)
- Obscene Publications Act (1959 & 1964)
- Counter-Terrorism and Security Act (2015)

## 7 Breaches of Security

7.1 Any individual suspecting that the security of a computer system has been, or is likely to be, breached should inform the IT Service Desk immediately. They will advise on what steps should be taken to avoid incidents or minimize their impact, and identify action plans to reduce the likelihood of recurrence.

7.2 In the event of a suspected or actual breach of information security, IT Security, with or without consultation with the relevant department, may require that any systems suspected of being compromised are made inaccessible.

7.3 Where a breach of security involving either computer or paper records relates to personal information, the University Data Protection Officer must be informed, as there may be an infringement of the Data Protection Act 1998.

7.4 All physical security breaches should be reported to the University's Security Office.

## 8 Policy Awareness and disciplinary procedure

8.1 This policy will be provided to all new and existing staff, students and members of the University. All other users of the University's information systems will be advised of the existence of this policy, which will be made available on the University website.

8.2 All users are required to familiarise themselves with this policy and comply with its requirements.

8.3 Failure of an individual student or member of staff to comply with this policy may lead to the instigation of disciplinary procedures up to and including dismissal and, in certain circumstances, legal action may be taken. Failure of other users to comply may lead to revocation of access, the cancellation of a contract and, in certain circumstances, legal action. The University may refer the user to the police where it reasonably believes a crime has been committed and will co-operate fully with any police investigations.

## 9 Governance

9.1 Responsibility for the production, maintenance and communication of this top-level policy document and all sub-policy documents lies with the University's IT Security Manager.

9.2 This top-level policy document has been approved by the Information Technology Governance Group (ITGG). Substantive changes may only be made with the further approval of this group. Responsibilities for the approval of all sub-policy documents is delegated to the Information Security Group (ISG). Before approving any sub-policy the ISG will consult with the ITGG, where necessary.

9.3 Each of the documents constituting the Information Security Policy will be reviewed annually. It is the responsibility of the IT Security Manager to ensure that these reviews take place. It is also the responsibility of the IT Security Manager to ensure that the policy set is and remains internally consistent.

9.4 Changes or additions to the Information Security Policy may be proposed by any member of staff, via their Head of School or Department to the IT Security Manager.

9.5 Any substantive changes made to any of the documents in the set will be communicated to all relevant personnel.

## 10 Policy Set

The complete Information Security Policy document set comprises of:

| Policy Name | ID | Status |
|---|---|---|
| Information Security | ISP-001 | Live |
| Acceptable Use | ISP-002 | Live |
| Business Continuity | ISP-003 | *In progress – due June 2017* |
| Disaster Recovery | ISP-004 | *In progress – due July 2017* |
| Incident Management | ISP-005 | *In progress – due August 2017* |
| User Account Management | ISP-006 | TBC |
| Mobile Device | ISP-007 | TBC |
| Network Configuration | ISP-008 | TBC |
| Physical Security | ISP-009 | TBC |
| Application Security | ISP-010 | TBC |
| System Configuration & Maintenance | ISP-011 | TBC |
| Penetration Testing | ISP-012 | Live |

## 11 Associated Policies and Documents

The following University of London policies support and provide additional context to this policy:

- Data Protection Policy
- Freedom of Information Policy
- Data Classification Policy
- Records Management Policy
- Risk Management Policy
- Social Media Policy
- Research Data Management Policy

## 12 Version Control

| Date | Version | Purpose/Change | Author |
|---|---|---|---|
| 27/04/2016 | 0-1 | Initial draft | IT Security & Business Continuity Manager |
| 31/05/2016 | 0-2 | Consultation draft – to working group | IT Security & Business Continuity Manager |
| 09/06/2016 | 0-3 | Consultation draft – to working group | IT Security & Business Continuity Manager |
| 14/07/2016 | 1-0 | Final version – approved by the Information Technology Governance Group (ITGG) | IT Security & Business Continuity Manager |