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

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 o will inat( )-9.17 709.78 Tm[ation.

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

9 Governance

9.1 Responsibility for the production, maintenance and communication of this top-level policy document and all sub-policy documents lies [illegible]

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

12 Version Control

Date	Version	Purpose/Change	Author
27/04/2016	0-1	[redacted]nitial draft	IT Security & Business Continuity Manager
31/05/2016	0-2	Consultation draft t to working group	IT Security & Business Continuity Manager
09/06/2016	0-3	Consultation draft t to working group	