Information Security Policy

Purpose

1. The confidentiality, integrity and availability of information, in all its forms, are fundamental to the ability of City University London to teach, undertake research and otherwise conduct its business. Failure to secure information increases the risk of financial and reputational losses from which it may be difficult to recover.

2. This information security policy provides the overall framework within which the security of information will be maintained and promoted across the University.

3. A University comprises a rich and diverse set of information assets, each of which have their own security requirements: a “one size fits all” approach to securing these assets is not appropriate. This policy recognises this, and sets high-level requirements and duties on all “information owners”, and authorises subsidiary information security regulations, standards, and procedures which shall be considered part of this information security policy and shall have equal importance.

4. It also defines relevant roles and responsibilities that relate to the implementation of this policy.

Scope

5. This policy is applicable to all staff, students, other members of the University and to third parties who interact with the information held by the University in all its forms and its related information systems. This includes, but is not limited to, any systems or data attached to the University computer or telephone networks, systems supplied by the University or communications sent to or from the University.

Policy Statement

6. The University is committed to the security of its information and information systems:
   - **Maintaining confidentiality**: only allowing authorised access to information;
   - **Ensuring integrity**: preventing unauthorised modification of information;
   - **Assuring availability**: critical information must be accessible when it is needed;
   - **Ensuring legal compliance**: making sure that the University is compliant with all relevant legislation.

7. This will be achieved by publishing additional, subsidiary information security regulations which will implement appropriate controls to ensure the confidentiality, integrity and availability of information from accidental and deliberate acts.

8. In addition various codes of conduct, guidance and best practice notes, etc., relating to specific areas will also be published.

9. To determine the appropriate levels of security measures applied to information systems, a process of risk assessment and periodic reviews shall be carried out for each service or system to identify the probability and impact of security failures by the person responsible for the information contained

---

1 E.g. Teaching & Learning materials, proprietary research data, financial or Personal information, etc.
within that system.

10. An information security steering group, comprising management representatives from relevant parts of the organisation, shall coordinate the implementation of information security controls and approve subsidiary policies.

11. This policy, and its subsidiaries, shall be reviewed and updated regularly to ensure that they remain appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations by the Information Security Group. Additional regulations may be created to cover specific areas as required.

Roles and Responsibilities

12. The CIO has the overall responsibility for the implementation of this policy in the University, with day-to-day responsibility for delegated to the Information Security Manager.

13. The CTO is jointly responsible for ensuring that appropriate security measures are put in place for centrally managed IT systems in conjunction with the Service Owner.

14. Academic staff (both teaching and research) and students have individual responsibility for any information which comes into their possession as a consequence of their relationship with the University.

15. The Information Security Manager is responsible for this and subsequent information security policies and will provide specialist advice throughout the University on information security issues.

16. The Head of Compliance is responsible for Data Protection and Freedom of Information issues.

17. The Head of Security is responsible for physical aspects of security and will provide specialist advice throughout the University on physical security issues.

18. All staff, students, visitors and third parties related to the School must handle information in accordance with this policy and any relevant local legislation, either in the UK, EU or where ever the information or data are being held or processed.

19. The University will establish and maintain appropriate contacts with other organisations, law enforcement authorities, regulatory bodies, and network and telecommunications operators in respect of its information security policy.

Reporting

20. Any actual or suspected breach in information security must be reported to the Information Security Manager in a timely manner, who will take appropriate action and inform the relevant authorities.

Disciplinary Procedure

21. Failure to comply with this policy, or its subsidiary regulations, may result in disciplinary action, via the appropriate HR process in the case of staff or the Student Disciplinary Regulations for students.