

INFORMATION SECURITY MANAGEMENT POLICY

Security Classification	Level 4 - PUBLIC
Version	1.3
Status	APPROVED
Approval	SMT: 27 th April 2010 ISC: 28 th April 2010 Senate: 9 th June 2010 Council: 23 rd June 2010
Life	3 Years
Review	<ul style="list-style-type: none">• Annual Management Review• Full review by June 2013
Owner	The Assistant Secretary

Foreword to Information Security Policy

In the age of the 'knowledge economy' and 'information society' information in all its forms has become, more than ever before, the currency of everyday interactions, debate, enlightenment, education, commerce, controversy and concern.

In acquiring this level of importance in society information has naturally accrued a culture of rights and responsibilities which has in many cases - such as the protection of personal data, and intellectual property and the need for public transparency - been formalised by both legislation and regulatory requirements to which the IOE is subject.

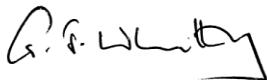
Where information is held by Institutions we are expected to ensure that we have proper regard to its:

- Confidentiality – to the extent that the nature of the information requires this.
- Integrity - so that confidence can be had in the information's origin, content, relevance and accuracy.
- Availability - such that appropriate individuals and groups can access, update, read, interpret or monitor the information.

Information security management is the means by which we ensure that we are taking account of these three factors.

The aim of this policy to ensure that staff and students of the IOE all understand the importance of Information Security Management as defined above and in the policy as it relates to the information they gather, process and store and the legal and ethical responsibilities that are incumbent on them both as individuals and as members of the IOE staff.

With this aim in mind I commend this policy to you and ask to have proper regard to it in your daily working lives.



Professor Geoff Whitty
Director
Institute of Education, University of London
November 2010

Contents

1. Policy	3
2. Scope	4
3. Definitions	4
4. Information Security Principles	5
5. Legal and Regulatory Obligations	6
6. Information Classification	8
7. Roles and Responsibilities	9
8. Compliance, Policy Awareness and Disciplinary Procedures	10
9. Incident Handling	10
10. Supporting Policies, Codes of Practice, Procedures and Guidelines	11

1. Policy Statement

1.1 Information is vital to the success of the Institute of Education, University of London (IOE). How information is acquired, processed and shared, both on an academic and a business level, defines critical components of the Institute's stated mission. Behind all the Institute's activities lies the critical requirement for effective data security to ensure the confidentiality, integrity and availability of its data and information systems.

1.2 This information security management policy outlines the IOE's approach to information security management. It provides the framework for describing the guiding principles and responsibilities necessary to safeguard the security of the Institute's information systems. These principles responsibilities are set out in this policy and supporting policies, codes of practice, procedures and guidelines.

1.3 The IOE is committed to a robust implementation of Information Security Management. It aims to ensure the confidentiality, integrity and availability of its data by adherence to the principles defined in this policy, which will be applied to all of the physical and electronic information assets for which the IOE is responsible.

1.4 The IOE is also specifically committed to preserving the confidentiality, integrity and availability of documentation and data supplied by, generated by and held on behalf of third parties pursuant to the carrying out of work agreed by contract in accordance with the requirements of ISO 27001: 2005 "*Information technology –security techniques – information security management systems (ISMS) – requirements*".

1.5 These commitments are made in the recognition that adherence to these principles is consistent with the mission and values of the IOE and critical to its core business; strategic plans; and legal, regulatory and contractual requirements.

1.6 These commitments will be embedded within the IOE's strategic and business planning and its risk management, major incident recovery and business continuity arrangements.

1.7 To meet the requirements of the ISO27001 for documentation and data supplied by, generated by and held on behalf of third parties pursuant to the carrying out of work agreed by contract, the IOE will establish and maintain a specific Information Security Management System (ISMS). This ISMS will be subject to regular, systematic review and improvement and will be embedded in the IOE's strategy and risk management framework. For information assets falling within the scope of the ISO27001, a risk assessment, Statement of Applicability and risk treatment plan will identify how related risks are controlled.

2. Scope

2.1 This policy applies to all members of the IOE (staff, students, external members of statutory committees); visitors to the IOE; partners with and sub-contractors to the IOE; and any other authorized users of the IOE's information.

2.2 The policy relates to the use of all IOE-owned information assets (both physical and system based), to all privately owned systems when connected directly or indirectly to the Institute's network and to all Institute-owned and/or licensed or sanctioned software/data and equipment.

3. Objectives

3.1 The primary objectives of this policy are to:

- 3.1.1 Ensure the protection of all Institute information systems (including but not limited to all computers, networking equipment, software and data) and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems.
- 3.1.2 Make certain that users are aware of and comply with all current and relevant UK and EU legislation.
- 3.1.3 Provide a safe and secure information systems working environment for staff, students and any other authorised users.
- 3.1.4 Make certain that all the Institute's authorised users understand and comply with this policy and any other associated policies, and also adhere to and work within the relevant codes of practice.
- 3.1.5 Protect the Institute from liability or damage through the misuse of its information systems facilities.
- 3.1.6 Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data that they handle.

4. Definitions

- **Data:** 'Raw' or undifferentiated information components. Often used interchangeably with the word 'Information'.
- **Information:** Data on its own carries no meaning. Information is data that has been interpreted been given or and taken on a meaning. Sometimes used interchangeably with the term 'data'.
- **Record:** an account in permanent form, especially in writing, preserving knowledge or information or data about facts or events

- **Information Security:** preservation of Confidentiality and Integrity and provision of Availability of information. Additionally refers to other properties, such as authenticity, accountability, non-repudiation, and reliability.
- **Confidentiality:** the prevention of the availability and disclosure of information to unauthorised individuals, entities or processes.
- **Integrity:** the safeguarding of the accuracy and completeness of (information) assets.
- **Availability:** The accessibility and usability of information upon demand by an authorised entity.
- **Information assets:** information or data and the media and systems upon which they are recorded for which the IOE is responsible.
- **Information Security Incident:** an event or series of events that have a significant probability of compromising business operations and threatening information security.

5. Information Security Principles

5.1 The following eight information security principles provide overarching governance for the security and management of information at the IOE.

- i. Information should be classified according to an appropriate level of confidentiality, integrity and availability (see *Section 7. Information Classification* and Section 5 of the *Data Security Policy*) and in accordance with relevant legislative, regulatory and contractual requirements and IOE policy (see *Section 6. Legal and regulatory Obligations*).
- ii. Staff with particular responsibilities for information (see *Section 8. Roles and Responsibilities*) are responsible for ensuring the classification of that information; for handling that information in accordance with its classification level; and for any policies, procedures or systems for meeting those responsibilities.
- iii. All users covered by the scope of this policy (see *Section 2. Scope*) must handle information appropriately and in accordance with its classification level.
- iv. Information must be complete, accurate, timely and consistent.
- v. Information should be both secure and available to those with a legitimate need for access in accordance with its classification level.
- vi. Information will be protected against unauthorized access and processing in accordance with its classification level.
- vii. Information will be protected against loss or corruption.
- viii. Breaches of this policy must be reported (see *Sections 9. Compliance* and *10. Incident Handling*).

6. Legal & Regulatory Obligations

6.1 The Institute of Education has a responsibility to abide by and adhere to all current UK and EU legislation as well as a variety of regulatory and contractual requirements. Relevant legislation includes:

- The Computer Misuse Act 1990
- Data Protection Act 1998
- The Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Copyright, Designs and Patents Act 1988
- Defamation Act 1996
- Obscene Publications Act 1959
- Protection of Children Act 1978
- Criminal Justice Act 1988
- Digital Economy Act 2010

6.2 A non-exhaustive summary of the legislation and regulatory and contractual obligations that contribute to the form and content of this policy is provided in Sections 6.3 to 6.7 below. Related policies (see Section 11.) will detail other applicable legislative requirements or provide further detail on the obligations arising from the legislation summarised below.

Relevant Legislation

6.3 The **Data Protection Act 1998** (DPA1998) provides a safeguard for personal privacy in relation to computerised or other systematically filed information; it regulates the use of personal data meaning info. about living human beings. It is an offence to process personal data except in strict accordance with the 8 principles of the DPA1998. Personal data must be:

1. Fairly and lawfully processed
2. Processed for limited purposes
3. Adequate, relevant and not excessive
4. Accurate and up to date
5. Not kept for longer than is necessary
6. Processed in line with your rights
7. Secure
8. Not transferred to countries outside the EEA without adequate safeguards

6.4 The **Freedom of Information Act 2000** (FOIA2000) is a general right of public access to all types of recorded info. held by public authorities in order to promote a culture of openness and accountability.

6.5 The **Computer Misuse Act 1990** defines offences in relation to the misuse of computers as:

1. Unauthorised access to computer material.
2. Unauthorised access with intent to commit or facilitate commission of further offences.
3. Unauthorised modification of computer material.

Regulatory & contractual obligations

6.6 The **Model Financial Memorandum between HEFCE and institutions (2008/19)** requires the Institute to have effective arrangements for the management and quality assurance of data submitted to HESA, HEFCE and other funding bodies. This includes:

1. Student data
2. Staff Data
3. Financial Data
4. Estates Data

6.7 Many **government and related contractors** of our services now require compliance with the international standard ISO 27001: 2005 *“Information technology - security techniques – information security management systems (ISMS) – requirements”*.

7. Information Classification

7.1 The following table provides a summary of the information classification levels that have been adopted by the IOE and which underpin the 8 principles of information security defined in this policy. Detailed information on defining information classification levels and providing appropriate levels of security and access is provided in the Data Security Policy.

Security Level	Definition	Examples	FOIA2000 / DPA1998 status
1. Confidential	Normally accessible only to specified members of IOE staff	Sensitive personal data; salary information; bank details; draft research reports; passwords	Subject to significant scrutiny in relation to appropriate exemptions/ public interest and legal considerations.
2. Restricted	Normally accessible only to specified members of IOE staff or the student body	Personal Data; reserved committee business; draft reports, papers and minutes; systems;	Subject to significant scrutiny in relation to appropriate exemptions/ public interest and legal considerations.
3. Protected	Normally accessible only to members of the IOE staff or the student body	Internal correspondence, final working group papers and minutes, committee papers, information held under license	Subject to scrutiny in relation to appropriate exemptions/ public interest and legal considerations
4. Public	Accessible to all members of the public	Annual accounts, minutes of statutory and other formal committees, pay scales etc. Information available on the IOE website or through the IOE's Publications Scheme.	Freely available on the website or through the IOE's Publication Scheme.

8. Roles & Responsibilities

8.1 Members of the Institute (See Section 2 Scope): all members of the IOE will be users of information. This carries with it the responsibility to abide by this policy and its principles and relevant legislation, supporting policies, procedures and guidance. No individual should be able to access information to which they do not have a legitimate access right. Systems will be in place to ensure that this is the case, but notwithstanding this, no individual should knowingly contravene this policy, nor allow others to do so.

8.2 Data Guardians: Many members of the IOE will have specific or overarching responsibilities for preserving the confidentiality, integrity and availability of information. These include:

8.2.1 Principal Investigators/ Project administrators: are responsible for the information security of information produced, provided or held in the course of carrying out research, consultancy or knowledge transfer activities. This including user administration (access rights, security mechanisms) and information administration (access controls, backup, retention and disposal).

8.2.2 Heads of Department/ Systems administrators: are responsible for the information systems (e.g. HR/ Registry/ Finance/ CRM) manual and electronic that support the IOE's work. Including user administration (access rights, security mechanisms) and information administration (access controls, backup, retention and disposal).

8.2.3 Heads of Department/ Section/ Line managers: are responsible for specific area of IOE work including all the supporting information and documentation that may include working documents/ contracts/ staff or student information.

8.2.4 Information Services Staff: are responsible for ensuring that the provision of the IOE's IS infrastructure is consistent with the demands of this policy and current good practice.

8.2.5 Senior Management: the Senior management of the IOE have overarching responsibility for ensuring that the IOE's commitment to this policy is met.

8.2.6 Directorate: the Director of Administration is responsible for the review, development and enforcement of this policy and for ensuring that appropriate action is taken in the event of a security incident or non-compliance that may result in a security incident.

9. Compliance, Policy Awareness and Disciplinary Procedures

9.1 Compliance with this policy and related policies will be enforced according to the IOE's Conduct Policy and Procedures (for staff) and Code of Conduct (for students).

9.2 In the case of a contractor failing to comply with this policy the result may be that the contract with the 3rd party is cancelled and where appropriate reported to the relevant authorities, including the police.

9.3 Any security breach of the Institute's information systems could lead to the possible loss of confidentiality, integrity and availability of personal or other confidential data stored on these information systems. The loss or breach of confidentiality of personal data is an infringement of the Data Protection Act 1998 and may result in criminal or civil action against the Institute. The loss or breach of confidentiality of contractually assured information may result in the loss of business, financial penalties or criminal or civil action against the Institute. Therefore it is crucial that all users of the Institute's information systems adhere to the Information Security Management Policy and its support policies as well as the Institute's Data Protection Policy.

9.4 A copy of this policy will be distributed to all new members of staff by the Human Resources Department; to all new students by the Registry and to all contracted services by the contracting department. All current staff, students and other authorised users will be informed of the existence of this policy and the availability of supporting policies, codes of practice and guidelines.

10. Incident Handling

10.1 If a member of the University (staff or student) is aware of an information security incident (see Section 2. Definitions) then they must report it to the Assistant Secretary/ Records manager in the first instance or failing that the Director of Administration, or use the IOE's Public Interest Disclosure (whistleblowing) policy.

The Assistant Secretary/ Records Manager Directorate Institute of Education, 20, Bedford Way, London, WC1H 0AL T: 020 7612 6008; F: 020 612 6059; E: matthew.grigson@ioe.ac.uk or recordsmanager@ioe.ac.uk	Director of Administration Directorate Institute of Education, 20, Bedford Way, London, WC1H 0AL T: 020 7612 6012; F: 020 612 6059; E: b.morris@ioe.ac.uk
---	--

10.2 In the event of a suspected or actual security breach Information Services or States and Facilities may, after consultation with the relevant head of department/faculty, authorise action to remove or restrict access to IOE systems, facilities and information or anything else deemed reasonable to secure information for which the IOE is responsible.

11 Supporting Policies, Codes of Practice, Procedures and Guidelines

11.1 Supporting policies have been developed to strengthen and reinforce this policy statement. These, along with associated codes of practice, procedures and guidelines are published together and are available for viewing on the Institute's website. All staff, students and any third parties authorised to access the Institute's network are required to familiarise themselves with these supporting documents and to adhere to them in the working environment.

11.2 Supporting policies:

Policy 1: Data Protection Act 1998 Compliance

Policy 2: Electronic Messaging

Policy 3: Conditions of Use of the Information Systems (Draft 1)

Policy 4: 'Conditions of Use for Computer Users - Staff' form

Policy 5: 'Conditions of Use for Computer Users – Students' form

Policy 6: Data Security

Policy 7: Information Systems Monitoring

Policy 8: Remote Access & Mobile Working Policy

Policy 9: Desktop Computer Security Policy

Policy 10: Server Security Policy