

**UNIVERSITY OF LONDON
RECORDS MANAGEMENT MANUAL:
BEST PRACTICE PROCEDURE No. 13**

INFORMATION SECURITY AND RECORDS MANAGEMENT

1.0 What is information security?

1.1 Information is an asset which, like other important business interests, is of value to an organisation and therefore needs to be suitably protected.

1.2 Information security may be defined as the preservation of:

- **confidentiality:** protecting information from unauthorised access and disclosure;
- **integrity:** safeguarding the authenticity, accuracy and completeness of information and processing methods; and
- **availability:** ensuring that information and associated services are available to authorised users when required.

1.3 Information exists in many forms. It may be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Appropriate protection is required for all forms of information to ensure business continuity and to avoid breaches of statutory, regulatory or contractual obligations.

2.0 Why is information security needed?

2.1 Organisations and their information systems face security threats from a wide range of sources, including computer-assisted fraud, sabotage, vandalism, theft, fire or flood. Damage caused by breaches such as computer viruses and computer hacking is becoming increasingly common and sophisticated.

2.2 Dependence on information systems and services means that organisations are increasingly exposed and vulnerable to security threats; security issues were not always the primary consideration in system design.

3.0 How to establish security requirements

3.1 Risk assessment. Potential threats to assets should be identified, as should the possible security risks of following current practices. Expenditure on controls should be balanced against the harm likely to result from security failures. Non-monetary factors such as loss of reputation should also be taken into account.

3.2 Legal, statutory, regulatory and contractual requirements must be taken into account.

3.2 The principles, objectives and requirements for information processing that an organisation has developed to support its operations must be identified.

4.0 Information security starting point

4.1 Controls essential to an organisation from the legislative perspective (see Best Practice Procedure *No. 12 Freedom of Information Act 2000*) include:

- Guidelines on data protection and privacy of personal information.
- Safeguarding of institutional records.
- Clarification of intellectual property rights.

4.2 Controls considered to be common best practice for information security include:

- An information security policy document.
- Allocation of information security responsibilities.
- Information security education and training.
- A procedure for reporting security incidents.
- Business continuity management.

5.0 Tracking of records and security

5.1 The tracking of records and information usage within records systems is a security measure for organisations.

5.2 Tracking ensures that only those users with appropriate permissions are performing information tasks for which they have been authorised.

5.3 Tracking systems can range from a handwritten note to an automated transaction in an electronic document management system.

5.4 The degree of control of access and regulation of use depends on the nature of the business and the records generated.

5.5 All tracking systems, however, have to meet the test of locating any record within the appropriate time period and ensuring that all movements are traceable.

6.0 Electronic records and authenticity

6.1 All information, irrespective of the media on which it is stored, is vulnerable to loss or change, whether accidental or deliberate. To protect information stored electronically, security measures need to be developed and implemented to reduce the risk of a successful challenge to its authenticity. Security measures need to include:

- Digital signatures to protect the authenticity and integrity of electronic documents (the **Electronic Communications Act 2000** provides for legal recognition of electronic signatures and the process under which they are generated, communicated or verified).
- Scanning and storing electronic records and digitised documents according to BSI PD 0008:1999, *Legal admissibility and evidential weight of information stored electronically* to ensure their authenticity in the event of a legal challenge.

7.0 Classification of information for security purposes

7.1 Classifications should take account of business needs for sharing or restricting information, and the business impacts associated with such needs e.g. unauthorised access or damage to the information. Classification of records is a shorthand way of determining how this information is to be handled and protected.

8.0 Security of confidential information

8.1 **Personal data:** The University holds and processes information about employees, students, and other data subjects for academic, administrative and commercial purposes.

8.2 When handling such information, the University, and all staff or others who process or use any personal information, must comply with the Data Protection Principles which are set out in the Data Protection Act 1998.

8.3 Responsibilities under the 1998 Act are set out in the Guidelines available at: <http://www.london.ac.uk/238.html>

8.4 The Data Protection Officer is available to help with general data protection queries. If you hold or process (or intend to process) personal data, you should, if you have not already done so, inform the Data Protection Officer data.protection@london.ac.uk

8.5 Further advice on records and information management issues, in relation to the Act, is also available within Best Practice Procedure No. 2: *Legislation and records management* and Best Practice Procedure No. 5: *Data Protection Act 1998 - Procedure for answering requests for information*.

8.6 **Creation and maintenance of confidential data:** Security requirements remain consistent for all such records, irrespective of format. If a record contains confidential material, then it must be maintained and disposed of securely i.e. only authorised persons should be allowed access to it. For a list of the classes of information which may be confidential, please refer to the appendix, Best Practice Procedure No. 6: *Destruction of confidential paper records*.

8.7 **Security of confidential paper records:** Confidential records should carry an appropriate classification label; file titles should be worded so that confidential information (e.g. someone's address, phrases such as "vexatious litigant") is not included in the title.

8.8 A clear desk policy should be standard practice i.e. when the member of staff is out of the office, any confidential data should be removed from the desk top and locked away. Similarly, filing cabinets containing confidential material should be locked at all times when not in use.

8.9 A list of persons authorised to process confidential records should be maintained and regularly reviewed

8.10 Faxes may not be secure, so consider carefully before using to transmit confidential information.

8.11 Non-current records which need to be kept for a specified period should be transferred to a secure storage facility; if the University of London Records Management Store is used please refer to Best Practice Procedure No. 7: *Transfer of paper records to semi-current storage*. Security of records in transit should be ensured.

8.12 **Security of electronic records:** Access to confidential records should be password protected and authorisation levels clearly documented.

8.13 Workstations should be locked when not in use.

8.14 When using mobile computing facilities such as laptops, special care should be taken to ensure that confidentiality is not compromised and that back-ups and virus protection are guaranteed by IT.

8.15 Email is not always a secure medium and the University cannot guarantee its confidentiality. Staff should be aware of this when using email to transmit confidential information.

8.16 Any removable media such as tapes, microfilm, disks or cassettes should be stored in a safe, secure environment in accordance with the manufacturers' specifications.

8.17 **Destruction of confidential data:** All staff have a responsibility to consider security when disposing of information in the course of their work.

8.18 For destruction of material in paper format refer to Best Practice Procedure No. 6: *Destruction of confidential paper records*.

8.19 Special care must be taken with the destruction of e-records, as deleted information can often be reconstructed. Erasing and reformatting disks or personal computers with hard drives which contained personal data is likely to be insufficient. Destruction should be carried out in collaboration with the IT Support team, which will have the software tools to ensure that the data is removed. Overwriting should ensure all previous information has been removed, but this should only be executed by authorised staff.

8.20 All destruction should be carried out in accordance with the provisions of the relevant retention schedule for that information, allowing for an audit trail to be kept.

9.0 A selection of legislation relevant to information security

- Computer Misuse Act 1990
- Contempt of Court Act 1981
- Copyright, Designs and Patents Act 1988
- Data Protection Act 1998
- Defamation Act 1996 (libel)
- Human Rights Act 1998
- Freedom of Information Act 2000

A summary follows as an appendix to this Procedure.

University of London Records Manager

Approved 23/06/04; Reviewed: 7/7/06; 29/9/09

Appendix: Legislation relating to information security

Computer Misuse Act 1990

There are three criminal offences under this Act:

- "unauthorised access to computer material" (hacking);
- "unauthorised access to computer material with intent to commit or facilitate commission of further offences" (e.g., hacking into a computer in order to commit theft by redirecting funds to own bank account, or to access confidential information in order to facilitate a blackmail scheme);
- "unauthorised modification of computer material" (deliberate erasure or corruption of programs or data, including the introduction of a "worm" or "virus" into a computer).

Contempt of Court Act 1981

It is an offence to publish or distribute anything which may impede or prejudice **active** legal proceedings, either accidentally or deliberately.

Copyright, Designs and Patents Act 1988 (as amended)

This makes unauthorised copying of any copyright work (including records) an infringement of copyright, unless it is covered by one of the exemptions included in the Act. The consent of the copyright owner is required for the copying of copyright material. Where electronic records are involved the software as well as the content of the records may be subject to copyright, and the two may be owned by different parties. Software will attract copyright.

Data Protection Act 1998

The **Data Protection Principles** state that personal data shall be:

1. Obtained and processed fairly and lawfully, and shall not be processed unless specific statutory conditions are met.
2. Obtained only for one or more specified and lawful purposes, and not be further processed in any manner incompatible with those purposes.
3. Adequate, relevant, and not excessive in relation to the purposes for which they are processed.
4. Accurate and, where necessary, kept up to date.
5. Held no longer than is necessary for the purposes for which they were obtained.
6. Processed in accordance with the rights of Data Subjects, including the general rights to access information held about them and where appropriate to correct or erase it.
7. Kept securely and safely, with appropriate measures to prevent unauthorised or unlawful processing of the data.
8. Only transferred to a country outside the EEA if that country has an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of personal data.

Defamation Act 1996

What is libel? Libel consists of a defamatory statement or representation in permanent form, e.g., statements in books, articles, newspapers, letters, emails or on a Web page. Every repetition of the libel is a fresh publication. As a result, not only the author of an article, but also the editor, printer and publisher are potentially liable, although they may be able to rely on the defence of innocent dissemination.

What to do when libel is suspected: If you suspect that a libel has been published, using University resources, it must be dealt with as quickly as possible. In particular, if it is published on a Web page it must be removed from there immediately. The relevant Head of Responsibility Centre must be informed as quickly as possible.

Human Rights Act 1998

This Act incorporated the European Convention on Human Rights into English law. Of particular relevance are Article 8 of the Convention, which gives everyone a right to respect for their private and family life, their home and their correspondence, and Article 10, which grants everyone the right to freedom of expression.

Freedom of Information Act 2000

This Act requires public bodies to be accountable for the information that they produce. Security is vital to the maintenance of a record's integrity and, therefore, necessary to comply with the legislation.