

**UNIVERSITY OF LONDON  
RECORDS MANAGEMENT MANUAL:  
BEST PRACTICE PROCEDURE No. 2**

**LEGISLATION AND RECORDS MANAGEMENT**

**Section 1. Legislation affecting records disposal at the University of London**

The following Acts of Parliament have sections relevant to record keeping and disposal:

- **Health and Safety at Work Act 1974**
- **Sex Discrimination Acts 1975 and 1986**
- **Race Relations Act 1976**
- **Limitation Act 1980**
- **Companies Acts 1985 and 1989**
- **Financial Services Act 1986**
- **Copyright, Designs and Patents Act 1988**
- **Value Added Tax Act 1994**
- **Disability Discrimination Act 1995**
- **Civil Evidence Act 1995**
- **Data Protection Act (DPA) 1998**
- **Freedom of Information (FOI) Act 2000**
- **Electronic Communications Act 2000**

1.1 The **Health and Safety at Work Act 1974** and its associated Regulations stipulate statutory minimum retention periods for records relating to:

- Risk assessment (review + 3 years)
- Monitoring of working environments (creation + 40 years)
- Control of and use of hazardous substances (file closure + 40 years)
- Monitoring of employees' health (creation + 40 years)
- Accident books (completion of book + 3 years)
- Accident/dangerous occurrence report forms (date of occurrence + 3 years)
- Categorising and disposal of waste (creation + 3 years)

1.2 The **Sex Discrimination Acts 1975 and 1986** recommend minimum retention periods for records relating to:

- Advertising of vacancies (filling of vacancy + 6 months)
- Job applications:
  - successful (transfer to staff personnel file)
  - unsuccessful (filling of vacancy + 6 months)

1.3 The **Race Relations Act 1976** recommends minimum retention periods for records relating to:

- Advertising of vacancies (filling of vacancy + 6 months)
- Job applications:
  - successful (transfer to staff personnel file)

- unsuccessful (filling of vacancy + 6 months)
- Ethnic monitoring questionnaire/reports (creation + 5 years)

1.4 The **Limitation Act 1980** recommends minimum retention periods for some financial records, contracts, product liability, some court actions, and personnel records as follows:

- Complaints (settlement of dispute + 6 years)
- Appeals (settlement of dispute + 6 years)
- Disciplinary hearings against staff (settlement of case + 6 years unless merged with staff personnel file)
- Staff personnel files (termination of employment + 6 years)
- Reporting and investigation of accidents and dangerous occurrences (date of accident + 40 years)
- Procurement records (e.g. tenders):
  - successful: termination of supply contract + 6 years
  - unsuccessful: creation + 1 year
- Lettings of student accommodation (termination of agreement + 6 years)
- Hiring out of conference facilities (termination of agreement + 6 years)
- Private hire agreements (termination of agreement + 6 years)
- Insurance policies (termination of policy + 6 years)
- Insurance claims (settlement of claim + 6 years)
- Conduct of testing, maintenance and statutory inspections and any necessary action (life of plant/equipment + 6 years)
- Maintenance schedules (creation + 2 years)
- Inspection certificates (creation + 6 years)
- Repair reports (life of plant/equipment + 6 years)
- Payroll payments (creation + 6 years)
- Share certificates (disposal of shares + 6 years)
- Investment portfolio reports (permanent)
- Control of disclosure of intellectual property (disclosure + 6 years)
- Administration of intellectual property agreements (termination of agreement + 6 years)
- Intellectual property agreements (termination of agreement + 6 years)
- Claims of infringement of intellectual property rights (settlement of claim + 6 years)

1.5 The **Companies Acts 1985 and 1989** stipulate statutory minimum retention periods for:

- Company accounts (creation + 6 years)
- Records of dissolved companies (dissolution + 10 years)

1.6 The **Financial Services Act 1986** and related regulations stipulate a statutory minimum retention period for:

- Salary advices (current financial year + 3 years)

1.7 The **Copyright, Designs and Patents Act 1988** (as amended) requires clear knowledge of the ownership of copyright in records before any outside person may copy any part of the record. 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.

1.8 The **Value Added Tax Act 1994** stipulates a statutory minimum retention period for:

- Purchase orders (creation + 6 years)
- Delivery and goods received notes (creation + 6 years)
- Income and expenditure accounts (creation + 6 years)
- Management of bank accounts (creation + 6 years)
- Assessment of tax liabilities (current tax year + 6 years)
- Submission of tax returns (current tax year + 6 years)

1.9 The **Disability Discrimination Act 1995** recommends minimum retention periods for records relating to:

- Advertising of vacancies (filling of vacancy + 6 months)
- Job applications:
  - successful (transfer to staff personnel file)
  - unsuccessful (filling of vacancy + 6 months)

1.10 The **Civil Evidence Act 1995** has resolved many of the problems of legal admissibility of evidence generated by or held on computers, by shifting the argument away from admissibility to the evidential value or weight of a document. A court will still need to be satisfied as to the authenticity of the document, and procedures need to be in place to prove this.

1.11 The **Electronic Communications Act 2000** provides for legal recognition of electronic signatures and the process under which they are generated, communicated or verified.

1.12 The **Freedom of information Act 2000** complements the **Data Protection Act 1998**, which gives individuals a right of access to information about themselves and provides for its processing by an organisation. FOI provides a route of access to all other information and consequently has a greater scope than DPA. Together the two Acts provide routes of access to all information held by the University.

1.13 The Acts have far-reaching implications for all aspects of information and records management throughout the University and are discussed separately in Section 2 below.

For further information see also <http://www.london.ac.uk/238.html> and <http://www.london.ac.uk/foi.html>.

## 2. Access to information legislation: the Data Protection Act and the Freedom of Information Act

2.1 **The Data Protection Act 1998:** The eight 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. In the case of 'sensitive personal data' (defined as data relating to racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health, sexual life,

and criminal offences and proceedings), at least one of the specific statutory conditions in Schedule 3 of the Act must also be 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 purpose(s) 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, and against accidental loss or destruction of, or damage to, 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.

## 2.2 Definition of terms under the Act:

- "Data" means information which -
  - (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,
  - (b) is recorded with the intention that it should be processed by means of such equipment,
  - (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system.
- "Relevant filing system" means any set of information relating to individuals that is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.
- "Personal data" means data which relate to a living individual who can be identified-
  - (a) from those data, or
  - (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual;
- "Data subject" means an individual who is the subject of personal data;
- "Processing", in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including -

- (a) organisation, adaptation or alteration of the information or data,
- (b) retrieval, consultation or use of the information or data,
- (c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
- (d) alignment, combination, blocking, erasure or destruction of the information or data;

### 2.3 Aspects of the Act which affect record keeping and disposal include:

- Contracts with staff and third parties, which may relate to external records storage, data back-up or the destruction of confidential waste, should ensure environmental control, disaster planning and security are covered adequately.
- Storage facilities and retrieval and access procedures should ensure personal data are held securely and access provided on a controlled basis only. Security procedures should comply with the corporate information security policy or accepted external standards.
- Procedures for the protection of vital records and for disaster recovery should meet accepted standards.
- An inventory of all collections of personal data held by the organisation should be maintained. This will form the basis for notification and for compliance control within the semi-current records store after transfer.
- Retention policies and schedules should ensure that personal data are not held longer than necessary. As a general rule, personal data should be disposed of as a result of the routine application of retention schedules and not on an ad hoc basis. Schedules may provide for personal data to be further processed and kept indefinitely as archives for research purposes.
- Secure, controlled destruction of records is essential.
- All staff should be aware that the Act applies to data held by individuals, such as personal mailboxes and word-processed documents. Personal filing systems should be discouraged.
- E-mail is not a secure medium and should not be used to transmit information which may be subject to the DPA. Use of personal e-mail should be kept to a minimum. Any e-mails required for the corporate record should be saved into an electronic records system or relevant folder structure; ephemeral e-mails should be destroyed promptly.
- Is the person alive or dead? Assume a life span of 100 years if you do not know the individual's date of death as DPA only applies to the living.
- Personal responsibility: responsibility for compliance with the Act rests on the individual creating and processing the record.
- How to respond to requests for access to personal data: please refer to Best Practice Procedure No. 5: *Data Protection Act 1998 - procedure for answering requests for information*

#### 2.4 The Freedom of Information Act 2000: What does FOI mean for the public?

- It provides an opportunity to find out what publicly funded bodies do and how they do it.
- It means that those bodies will be made more accountable.
- It relates to all information held by the University.
- The Freedom of Information Act 2000 came into effect in 2005.

#### 2.5 Responding to non-routine requests for information made under the Act:

- There is a statutory right of access, subject to certain exemptions, to all information held by the University; the age of the record is irrelevant.
- Any request for information under FOI must be dealt with according to the provisions of the Act, irrespective of the motive for the request, as long as the request is made in permanent format. Any letter, e-mail or fax is therefore a potential FOI request.
- Applicants have the right to be told whether or not the organisation has the information requested and to have any such information communicated to her/him according to the provisions of the Act.
- A response to enquiries, including provision of the information if it exists, must be made within 20 working days.
- If the information has been destroyed, the University must show that it has been destroyed in accordance with good business practice (a retention schedule will be accepted as evidence of good practice).
- The University has a duty to provide advice and assistance to applicants and to communicate information in an appropriate manner.
- The University may charge for the cost of making copies of documents.
- Procedures must be in place for handling FOI requests, and these procedures must conform to the code and enquiry procedures (Section 45 of the Act). Requests must be managed so that in the event of a dispute the handling of a request or a refusal to provide information can be defended.
- There are exemptions e.g. if the information sought is personal data.
- The University is required to have a publication scheme, listing the organisation's routinely published information. The scheme must be in the public domain and readily accessible, stating whether or not the information is free and in what format it is kept.
- The more extensive the publication scheme, the less FOI enquiries the University will have to answer.

## 2.6 Minimum record keeping standards for compliance with the Act:

- A records and information management policy statement must be in place.
- The audit of integrated records and information management practices, including compliance with access to information legislation, should be established and maintained.
- Adequate resources should be allocated to support the records management function.
- Each organisation must document its activities and have systems that enable quick and easy retrieval of information. Without such systems, compliance with the legislation will be impossible.
- Records must be properly stored, protected from damage, and their content secured against unauthorised access.
- Tracking systems should be set in place to control the movement and location of records so that they can be easily retrieved.
- Systems should be in place for the controlled retention and disposal of records, comprising:
  - preparation of records retention schedules;
  - creation of procedures for implementing and auditing the retention schedules;
  - the making of appropriate arrangements for the preservation of records of enduring value;
  - creation of procedures for the timely and secure destruction of records no longer required for business purposes and not selected for preservation;
  - creation of a system for documenting all appraisal decisions to include information on records destroyed, retained or selected for preservation.
- A designated, named person must be responsible for implementation of the records management function.
- Adequate training programmes should be set up for staff to ensure that they understand the necessity for records management under FOI.

University of London Records Manager & Freedom of Information Officer

*Procedure approved 9/9/02; amended 1/11/02; 10/12/02; 17/12/02; 30/1/03; 16/7/06; 25/9/09; 22/10/09*