

LONDON DEANERY

DATA PROTECTION POLICY

Applicable to:	All Deanery Staff
Lead Department:	Corporate Services

INTRODUCTION

This Policy implements the requirements of the Data Protection Act 1998, which came into force on 1 March 2000. It supplements the Central University's Data Protection Policy which can be found in the Terms and Conditions of Service Booklet given to all staff. The Policy covers the Deanery's use of personal data, that is data about identifiable living individuals, and applies to some paper records as well as those held on computer. The Act gives individuals the right to find out what information is being held on them.

PURPOSE OF THIS POLICY

The Deanery is committed to managing personal information in a fair and responsible manner. The Policy provides a structure and guidance to help manage the Deanery's responsibilities and, in Appendix 1, includes the procedure for managing data access requests by individuals. The purpose of this document is to ensure that staff are aware of their responsibilities under the Data Protection Act and are able to process information and respond to access requests in line with legal requirements.

COVERAGE AND RESPONSIBILITIES

This Policy applies to all staff in the London Deanery. It applies to temporary and agency staff and people on secondment. It covers agents of the Deanery who as part of their role have access to personal data, for example members of STCs. Everyone has a responsibility to comply with and implement that Policy and the Personal Data Access Procedure. The Dean Director recognises her responsibilities as head of organisation and has appointed the Director of Corporate Services as the local Data Protection Officer to advise them of developments and oversee the operation of appropriate systems to ensure compliance with the law. The Deanery is registered with the Information Commissioner as part of the Central University of London organisation and the Director of Corporate Services works with the University of London's Data Protection Controller.

The Director of Corporate Services has established a group of Data Protection Co-ordinators from Departments to act as local contacts. Their responsibilities are to:

- Provide a co-ordinating point for Data Protection issues in their department
- Give basic advice to other members of the department

- Highlight any potential data protection issues arising from new developments
- Participate in a quarterly co-ordinating group for the Deanery

IT staff will implement and maintain appropriate measures to ensure the security and integrity of computerised personal data.

EIGHT DATA PROTECTION GOOD INFORMATION HANDLING PRINCIPLES

The law requires us to comply with the following eight principles on data handling. Data must be:

1. Fairly and lawfully processed

Individuals must be clear on the purpose for which data about them is being obtained. They should have been provided with or had access to:

- ~ the identity of the Data Controller (University of London - (LPMDE)
- ~ the name of the nominated representative - (Head of HR and Central Services)
- ~ purpose(s) of the data processing
- ~ any other relevant information necessary to ensure the individual understands andthat the process is fair

2. Processed for limited purposes

We must be clear from the beginning as to the purpose(s) for which we are collecting data. Having made that purpose clear, we cannot then use such data for other reasons for which we have not received consent.

3. Adequate, relevant and not excessive

This means that the information we keep should not be so insufficient that it becomes misleading. It should also be relevant to our information needs and we should only collect and store what is strictly required for those needs.

4. Accurate and where necessary up to date

We must keep our records up to date and check and correct errors when noticed or notified to us.

5. Kept no longer than is necessary for the stated purpose or purposes

Personal data cannot be kept indefinitely. The length that data is kept will depend on the purpose for which it is needed and will therefore vary for different types of data. Legal & Policy requirements affecting data storage are detailed in Appendix 2.

6. Processed in accordance with the rights of the data subject under the Act

We need to be aware of data subjects' rights and ensure we respond to these. See Appendix 3.

7. Processed using appropriate technical and organisational methods to ensure against unauthorised or unlawful processing of data and against accidental loss or destruction of, or damage to, personal data.

This Principles covers both appropriate IT systems including passwords, backups and

encryption, where appropriate, and processes and procedures to ensure that manual data is handled lawfully, is not viewed by unauthorised personnel and is locked away when not in use.

8. Prevented from being transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for personal data.

Certain exceptions may apply including where each data subject has given his or her consent to the transfer. If in doubt please seek advice from your local Data Protection Co-ordinator

Personal data covers both facts and opinions about the individual. It also includes information regarding the intentions of the data controller towards the individual.

DATA DISCLOSURE

Where data is disclosed to an individual, care must be taken to ensure that third party data is not inadvertently disclosed. Additionally, staff must not disclose data to third parties unless:

- The individual has given written consent
- We have a legal responsibility/right to disclose the information
- It is an emergency e.g. critical medical reasons

Where express consent is not present, the decision to disclose information must be taken by the Head of Department. Even where consent has been obtained or where there is a legal responsibility to disclose information, staff must accept only written requests for disclosure of information and satisfy themselves that the request does come from the source indicated. Any doubts must be raised with a line manager.

REVIEW

This Policy and its appendices will be reviewed regularly in the light of experience and developments in the law and Codes of Practice.

For further information contact:	Director of Corporate Services
Related Documents:	Freedom of Information Policy IT Acceptable Use Policy

APPENDIX 1

PROCEDURE FOR HANDLING DATA ACCESS REQUESTS

This procedure forms part of the Data Protection Policy of the Deaneries and should be interpreted in accordance with that Policy. The Procedure explains how to handle request for access to personal data made by individuals. If you are unclear about any aspect of the procedure you should contact your local Data Protection Co-ordinator (DPC) or the Director of Corporate Services (DoCS).

1. Requests for data access may come in various formats e.g. in person, over the phone, by letter or by e-mail. Individuals should be handed or sent the Data Access Request Form and asked to make a formal request. This should occur no later than 2 working days after the request has been received.
2. Completed forms must be sent to the DoCS. The DoCS will advise the DPC and the Head of Department of the application. The latter two individuals will take responsibility for handling the access request.
3. The DPC must ensure that evidence of identity has been provided and that this corresponds with information held by us on this individual. If there is any doubt, further enquiries may need to be made and additional information may be requested.
4. A fee of £10 will be charged for administration.
5. The Deanery has 40 days from receipt of adequate proof of identify and payment of the fee to provide information on the personal data held.
6. Care must be taken to ensure that third party data contained in the individual's data is not disclosed without seeking prior consent.
7. Information must be sent to an individual by recorded delivery and be accompanied by a covering letter which should explain:
 - ~ Whether personal information is being processed and for what purposes
 - ~ A description of the data
 - ~ Potential recipients of the data
 - ~ Source of the data
 - ~ Whether any automated decisions are being taken and the logic behind this
 - ~ Any codes used in the personal data must be explained if they may not be commonly understood.
8. Where a second request comes from the same individual, further disclosure need only occur if a 'reasonable interval' has occurred or where new information is available. Refusals must first be agreed with the DoCS.
9. Complaints concerning the application of this procedure must be addressed to the DoCS.

GUIDANCE ON RETENTION OF RECORDS

The destruction of records is an irreversible act, while the retention of records has resource implications. Decisions to destroy or archive information should be taken with care. The following is guidance on the minimum retention period for documents.

TRAINEE RECORDS

Trainee Records – keep full file for 6 years after completion of training. Summary file should be kept until the person reaches their 70th birthday.

EMPLOYMENT/RECRUITMENT RECORDS

Health & Safety: information concerning accidents, incidents or complaints which may lead to a Personal Injury Claim (including mental illness) must be kept for 3 years from the date of the accident.

Personal file: kept for 15 years after the employee has left. The file should be weeded out so that only key information required for references is available after 6 years.

Payroll – 6 years

Recruitment paperwork: complaints to an Employment Tribunal can, in exceptional cases, be allowed over a year after the recruitment episode. The recruitment records should be kept for one year. The details of the successful applicant's application etc. can be stored on the Personal File (see below).

References: References should be kept for unsuccessful candidates – 1 year. The details of the successful applicant's application etc. can be stored on the Personal File (see below).

Supervision/local staff files: should be kept for 3 years after the individual has left. If key documents are held on these files they should be extracted and added to the personal file.

Training Records: should be kept for 3 years after an employee has left.

FINANCIAL RECORDS

Accounts: Annual (final) – permanent

Accounts: Costs and working papers – 3 years

Accounts: 2 years for minor records e.g. pass books, paying-in-slips, cheque counterfoils, cancelled/discharged cheques bearing printed receipts, accounts of petty cash expenditure, travelling and subsistence accounts

Approved suppliers lists – 11 years (Consumer Protection Act 1987)

Audit reports: 2 years from completion of the audit

Bank Statements – 2 years

Bills, receipts and cleared cheques – 6 years

Budgets – 2 years

Creditor payments – 3 years

Estimates – 3 years

Expense claims – two years from completion of audit.

Income and expenditure journals – 6 years

Invoices – 6 years (The Limitation Act 1980)

GENERAL

Buildings and engineering works – permanently retained

Buildings – relating to occupation but not health & safety – 3 years

Contracts – 6 years if not sealed (The Limitations Act), minimum 15 years if sealed

Delivery notes – 1.5 years

Inspection reports – lifetime of installation e.g. boilers, lifts etc.

Software licences – lifetime of product

UNDERSTANDING THE ACT

THE RIGHTS OF INDIVIDUALS

1. The right of subject access

To find out about what information is held about themselves on computer and some paper records. This is known as the right of subject access.

2. The right of rectification, blocking, erasure and destruction

The right to apply to a court to order a data controller to rectify, block, erase or destroy personal details if they are inaccurate or contain expressions or opinions which are based on inaccurate data.

3. The right to prevent processing

To ask a data controller to stop or request that they do not begin processing relating to him or her where it is causing, or is likely to cause, substantial unwarranted damage or substantial distress to themselves or anyone else. However, this right is not available in all cases and data controllers do not always have to comply with the request.

4. The right to prevent processing for direct marketing

A data subject can ask a data controller to stop or not to begin processing data relating to him or her for direct marketing purposes. This is an absolute right.

5. The right to compensation

A data subject can claim compensation from a data controller for damage or damage and distress caused by any breach of the DPA. Compensation for distress can only be claimed in limited circumstances.

6. Rights in relation to automated decision-taking

An individual can ask a data controller to ensure that no decision which significantly affects them is based solely on processing his or her personal data by automatic means. There are, however, some exceptions to this.

PAPER FILES

The DPA covers information that is recorded as part of a "relevant filing system". This is described as a set of information in which the records are structured, either by reference to individuals or by reference to criteria relating to individuals, so that "specific information relating to a particular individual is readily accessible". This definition means that a significant amount of manual data falls under the scope of the DPA.

PROCESSING PERSONAL DATA

The concept of processing data includes 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, adaption or alteration
- (b) Retrieval, consultation or use
- (c) Disclosure of the information or data by transmission, dissemination or otherwise making available
- (d) Alignment, combination, blocking, erasure or destruction of the information or data

Personal data must be processed "fairly and lawfully". One of the following conditions must be met:

- ◆ the individual has given his or her consent to the processing
- ◆ the processing is necessary for the performance of a contract with the individual
- ◆ the processing is required under a legal obligation
- ◆ the processing is necessary to carry out public functions
- ◆ the process is necessary in order to pursue the legitimate interests of the data controller or third parties (unless it could prejudice the interests of the individual).

PROCESSING SENSITIVE PERSONAL DATA

The DPA includes the following as personal sensitive data: racial or ethnic origin; political opinions; religious or other beliefs; trade union membership; health; sex life; criminal proceedings or convictions. Sensitive data can only be processed under strict conditions:

- ◆ having the explicit consent of the individual i.e. in writing
- ◆ being required by law to process the data for employment purposes
- ◆ needing to process the information in order to protect the vital interests of the data subject or another
- ◆ dealing with administrative justice or legal proceedings