

UNIVERSITY OF LONDON

DATA PROTECTION GUIDELINES

Revised September 2007

1. Introduction

The University, like other large organisations, needs to handle personal data about individuals in order to carry out its work and fulfil its obligations to members of staff and students. The law governing the way in which such data should be used or processed was modified a few years ago, following the issue of an EU Directive. The current rules are set out in the Data Protection Act 1998, which came into effect on 1 March 2000.

The 1998 Act in many ways mirrors the previous 1984 Act, but the rights of individuals have been expanded, and the legislation has been extended to cover manual data, and not just the computerised data which were covered by the earlier law. The Act includes some complex transitional provisions which delayed the effective date of some parts of the Act for certain limited purposes until 24 October 2001 or, in the case of some manual data, until 24 October 2007. However, it would be good practice for the University to adopt a policy on the basis that all sections of the Act are fully in force, and this assumption has been made in the following guidance.

It must be emphasised that this guidance is a simplified version of rather complex legal rules and is primarily intended to assist staff. It does not deal with those provisions in the legislation which are unlikely to have a direct impact on the University. The purpose of the law in this area is to protect the rights of individuals with regard to the personal data which others ('data controllers') hold on them. In many cases common sense will lead to the right conclusion, if due attention is paid to the broad purpose of the legislation. In cases of doubt, refer to the University's Data Protection Officer (email: data.protection@london.ac.uk).

2. Definitions

The law governs the processing of personal data. All these terms are defined in the 1998 Act.

- 'Data' includes both manual and automated information, such as information held on a computer, video surveillance and CCTV material, and retrievable data held on telephone or fax machines. Manual information is covered by the Act if it forms part of a 'relevant filing system', that is a system structured so that specific information relating to an individual is readily accessible. Health records of individuals, prepared by health professionals in connection with the care of those individuals, fall within the definition even if they are informal, manual notes.

In the *Durant* case in 2003 the Court took the view that the Act intended to cover manual files "only if they are of sufficient sophistication to provide the same or similar ready accessibility as a computerised filing system". This means that any manual filing system which, for example, requires a search through files to check whether information qualifying as personal data of the individual making a request for information is present in the files, would not be considered comparable to a computerised search and would not qualify as a 'relevant filing system'. On the other hand, personnel and manual files which use individuals' names or unique identifiers as file names and which are sub-divided/indexed to allow retrieval of personal data without a manual

search are likely to be considered to be held ‘in a relevant filing system’ for the purposes of the Act. In the light of the *Durant* judgment, the Information Commissioner has stated that it is likely that very few manual files will be covered by the provisions of the Act.

- ‘Personal data’ means data relating to a living individual (referred to in the Act as a ‘data subject’) who can be identified from the data, or from the data together with other information in the possession of the data controller. It includes expressions of opinion about the individual and data setting down the intentions of the data controller (or anyone else) relating to that individual.

In the *Durant* case the Court provided further clarification on the nature of personal data. To fall within the definition ‘personal data’ have to be biographically significant and also have to focus on the individual. This means that the inclusion of an individual’s name on a document will only be ‘personal data’ where its inclusion in the information affects the named individual’s privacy. Mere inclusion in a list of names, or incidental mention in the minutes of a meeting of an individual’s attendance at that meeting, for example, would not be considered sufficient.

- ‘Processing’ is very widely defined. It includes the holding of data and virtually every operation on the data from collection to destruction.

3. Notification

In order to process personal data, a ‘data controller’ such as the University has to inform the Information Commissioner and comply with the Act’s notification (registration) procedure. It is important that the University’s notification covers **ALL** processing activities. **Any processing which is not in accordance with our notified activities constitutes an infringement of the Act and is an offence, punishable by a fine.** The University’s Data Protection Officer deals with the Information Commissioner’s office regarding our notification. All new activities involving the processing of personal data should be reported to the Data Protection Officer for the central University’s Institutes and Activities so that we can ensure that they are encompassed by our current notification, or extend our cover if necessary.

The University’s notification covers all the central University administrative offices based at Senate House (including the Library) and at Stewart House, as well as the Institutes of the School of Advanced Study, University Marine Biological Station Millport, intercollegiate Halls of Residence, University of London Computer Centre, University of London Careers Group, University of London Union, University of London Housing Services and the London Deaneries. Individual Colleges of the University are separate legal entities and therefore have their own notifications. College DPOs should be consulted concerning data protection matters relating to personal data held at those institutions.

4. The Data Protection Principles

Personal data must be processed in accordance with the eight principles listed in the Act. The following paragraphs set out these principles and the action which the University and its staff should take to ensure compliance.

First Principle:- **Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:-**

- **at least one of the conditions in Schedule 2 is met, and**

- **in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met [see below]**

Second Principle:- Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes

Third Principle:- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed

Fourth Principle:- Personal data shall be accurate and, where necessary, kept up to date

Fifth Principle:- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes

Sixth Principle:- Personal data shall be processed in accordance with the rights of data subjects under this Act

Seventh Principle:- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data

Eighth Principle:- Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

5. The First and Second Principles: Fair and lawful processing

In accordance with the principle of fair and lawful processing, the University must first of all satisfy at least one of the conditions set down for the processing of the personal data, and secondly ensure that the processing is fair.

Satisfaction of conditions: There are several conditions set down in Schedule 2. In the case of the University the conditions most likely to be relevant are:

- the data subject has given consent to the processing
- the processing is necessary for the performance of a contract with the data subject or for taking steps, at the request of the data subject, with a view to entering a contract

The condition will also be satisfied if *inter alia* the processing is necessary to comply with a legal obligation, or to protect the vital interests of the data subject, or for the administration of justice or certain other public purposes.

An important new feature of the 1998 Act is the classification of certain data as ‘sensitive personal data’. These are 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. For the processing of sensitive personal data, a data controller must satisfy at least one of the extra conditions set out in Schedule 3. In the case of the University the conditions most likely to be relevant are:

- the data subject has given **explicit** consent to the processing
- the processing is necessary to enable the University to comply with its legal obligations under employment law

Fair and lawful processing: Personal data must be obtained openly, and the data subject must not be misled about the purposes for which the data are required. This means that the University must inform the individuals concerned of the identity of the data controller, and make clear the purposes for which the data are to be processed. This should include an explanation of any consequences of the processing and any likely disclosures. If there is any subsequent change in the specified purposes for which the data are to be used, and the new purpose is not one which is necessary for the fulfilment of a contract, then a new consent will have to be obtained from the individual.

The University collects a wide range of personal data relating to staff and students for its own purposes, and to meet external obligations. This information may eventually be transferred to third parties. All transfers of personal data which are made must comply with the Data Protection Principles, including the conditions outlined above. Where there is a need to obtain an individual's express consent for a transfer of personal data, such consent cannot be inferred from silence or from a failure to respond to a request for consent. Personal data must not be disclosed to unauthorised third parties, who will include family members, friends, local authorities, government bodies, and the police, unless disclosure is permitted by one of the exemptions in the Act (see 10 below).

Employment agencies or prospective employers may also contact the University to verify details about a student (for example, attendance records, exam results, and degree classifications). Disclosure of such information must comply with the principles described above and will normally require the consent of the student. Where, for example, a job is conditional on proof of qualifications, it is not unreasonable for applicants to provide physical evidence of these to the prospective employer or formal consent for that employer to verify the qualifications with the University.

It is likely that most of the processing of personal data undertaken by the University will be necessary for the performance of a contract with the individual, whether a contract of employment or a contract with a student. In entering into the contract, the individual may be deemed to have consented to the use of the data for purposes which are clearly related to the fulfilment of that contract. Such implied consent may be sufficient, but it must be specific and informed consent.

Individuals whose details appear on mailing lists and databases should have given their consent to the inclusion of their data and to the purposes for which the data are to be used. A general 'consent' notice stating that individuals' details will be held on a mailing list or database for certain named purposes (which must be specified), unless they object to the contrary, is acceptable. Express consent should be obtained from individuals before their data can be used for direct marketing purposes (see 7 below); and an individual is entitled to require a data controller not to use his or her data for direct marketing purposes.

The safest course is for the University to obtain explicit prior consent from the individual for **any** processing. This would best be done at the start by means of a simple declaration (or 'collection notice') in the contract of employment or student enrolment form. This should include a reference to each of the purposes for which it is envisaged that the data will be processed. Such collection notices may contain information about institutional and external use of staff and students' personal data. **In the case of sensitive personal data, express consent for processing is required in any event.**

6. The Third, Fourth, and Fifth Principles: Relevance, accuracy and retention

These principles are self-explanatory and relate to the adequacy and accuracy of the data, and the time for which they may be retained by the data controller.

Adequacy and relevance: One of the purposes of the third principle is to avoid the collection and retention of superfluous personal data. Candidates for jobs and prospective students should not therefore be asked to provide personal data beyond what is relevant for the immediate purpose, whether for employment or enrolment as a student. The University's application forms should be checked periodically to ensure compliance with this principle.

Accuracy: To maintain compliance with the fourth principle, a data controller such as the University is expected to take reasonable steps to ensure that data are accurate and up-to-date, and it may not be enough simply to rely on the state of the data as initially provided. Individuals have the right to have inaccurate data rectified or deleted. **It would therefore be prudent for the University to make periodic checks, perhaps annually, of the data which it holds and ask data subjects to confirm the accuracy of their data.** In the case of students this could be built into an annual re-registration procedure and, in the case of staff, through an annual reminder by Human Resources. A confirmation of the consents given under the first principle could be obtained at the same time.

Where requests are received from data subjects to amend or update their details, care should be taken to ensure that these amendments are actually made. Responsibility Centres might consider designating a key 'DPA' contact to whom all requests should be reported in the first instance. This should ensure that, should staff leave post, a central record of the request is maintained within the Responsibility Centre.

Retention: The University is entitled to hold at least basic records of former students (years attended, class of degree, etc) indefinitely, as former students may need proof of their qualifications at any time. For legal reasons, a full academic and conduct record should be retained for six years from the date of a student leaving an institution. Once that period has elapsed, the record can be reduced to a core record, that is, enough material to confirm the student's personal details, marks and degree class (and, if relevant, the process that led to that decision). All other material should be destroyed since it could be argued that it is excessive and irrelevant to the intended purpose. Sensitive data should also be removed at this stage.

Although data controllers must inform data subjects about any processing of their data, it would be impractical for institutions to contact all their former students and inform them that archive records are being kept about them or that information is being destroyed. The guidance from the Information Commissioner's office is that institutions need not attempt to contact all former students, but they should prepare a clear statement describing their archiving policy and archive holdings. This should be issued to any former student who makes an enquiry about data held, or requests a reference, transcript, certificate, or other information. If archival data are to be kept for research purposes (for example, assessing an institution's degree awarding performance), registration documents should make this purpose clear to incoming students and any archival data retained solely for the purpose of research should be anonymised.

In order to assist in responding to subject access requests, it might be helpful to consider drawing together all non-computerised records relating to a student at their point of departure for storage in a single archive. Departments might also consider compiling a list of the records which they hold and where they are located.

Staff records should not normally be retained for a period of longer than six years after the member of staff has ceased to be employed by the University.

The JISC *HEIs Function Activity Model (FAM) and Record Retention Schedule (RRS)*, as revised in 2002, [and previously known collectively as the *Study of the Records Lifecycle*] provides general guidance on best practice concerning the retention of records containing personal data which is available at:

http://www.jisc.ac.uk/whatwedo/themes/eadministration/recordsman_home/srl_structure.aspx

(Note: This is currently the subject of an updating project). More detailed and specific guidance for staff is provided in the latest approved versions of the records retention schedules of individual divisions/departments (copies available from departmental records management representatives, or from the Records Management Team (email: records.management@lon.ac.uk).

The recommended retention periods will have to be reconsidered in special cases, for example if a former student or member of staff is in dispute with the University.

7. The Sixth Principle: Individuals' rights

Individuals have a number of rights under the Act. These include a right to prevent processing likely to cause damage or distress, and a right to prevent processing for the purposes of direct marketing. Prior consent should be obtained from individuals before personal details such as their names and addresses are passed to others for direct marketing purposes. An individual may withdraw that consent, by notice in writing, at any time.

Subject Access Requests: Data controllers are obliged to supply data subjects with information about the data which they hold on them (including copies of the data) if requested to do so. Requests must be made in writing. The information requested must be supplied promptly, and no later than 40 days after the receipt of the request or, if later, receipt of the applicable fee. The University charges £10 (the maximum currently permitted) for this service. **The 40-day deadline is a statutory requirement**, and staff are reminded of the need to ensure that subject access requests are completed within this timescale.

Guidance for staff on the procedure for answering requests for information under the Act, together with an application form, may be found in the Records Management Procedures Manual (Best Practice Procedure No. 5) on the University Intranet (at <https://intranet.london.ac.uk/911.html>). A copy of the application form for making a subject access request is also attached as an Appendix to these Guidelines (see Appendix 1).

An individual has the right to prevent a data controller making decisions which significantly affect the individual (for example on matters such as the evaluation of performance or conduct) solely by means of the automatic processing of personal data. This right however does not apply where the decision is taken as part of a process which leads or may lead to the making of a contract with the individual or is taken in the course of performing such a contract, provided that the decision was made in response to a request from the individual or his interests have been properly safeguarded. If such decisions are taken, the individual has the right to be informed of the logic of the automated decision-making process (unless it is a trade secret).

Problems may arise if an individual asks to see copies of his or her own data, and the University

finds that it cannot comply with the request without at the same time disclosing information relating to a third party. In this case the University is obliged to comply with the request only if the third party has consented or if it is reasonable to respond to the request without such consent. In determining whether or not it is reasonable so to comply, the University is obliged to consider a range of factors, including any duty of confidentiality owed to the third party or any express refusal by the third party to give consent. In practice it may be possible to comply with the request by blocking out direct references to the third party or any information which would enable him or her to be identified.

Special rules apply to requests for the disclosure of examination marks. If a candidate makes a request for his examination marks before the results are announced, the period for compliance is five months from the date of receipt of the request (or receipt of the fee, if later), or forty days from the date of the announcement of the results, whichever is the sooner. Although marks must be revealed, there is an exemption for examination scripts, which do not have to be disclosed. Examiners' comments are not covered by the exemption. Comments recorded by an examiner about the performance of a candidate in an examination may be personal data and therefore available to a student making a subject access request. This is the case whether the comments are on the examination script or on a separate marking sheet. There is no exemption in the Act which permits withholding examination results from students who have outstanding debts to the University (such as examination or course fees). However, the release of examination results is not the same as the award of a degree or other qualification.

Confidential references given by a data controller such as the University are exempted from the disclosure requirements of the Act. The University is therefore not required to disclose the contents of such a reference to a member of its staff or a student who is the subject of the reference. The individual concerned however has the right to obtain a copy of the reference from the recipient. Referees must be aware that references may be disclosed to the individual, even though given to the recipient in confidence. As a matter of policy, in writing references, members of staff should only include statements which they would be prepared to make directly to the individual concerned.

8. The Seventh Principle: Security

The University is required to take proper care of the personal data which it holds and to prevent it being lost or corrupted or falling into unauthorised hands. The University must therefore undertake periodic checks to ensure that adequate security measures are in place. Managers should carry out an annual review of administrative, physical and technical safeguards for protecting personal information, held in both paper and computerised form, including a review of the security of offices, buildings, and (if applicable) portable devices such as laptops and personal digital assistants (PDAs).

Where data are stored electronically, the University will be required to update its security measures in line with technological advances. Technical measures which might be taken to ensure compliance with information security requirements include the use of encryption in the capture of sensitive personal data, especially in less secure environments. Advice should be sought from ULCC on technical computing matters.

Reasonable precautions must be taken to ensure security when transferring personal data in either hardcopy or electronic form. Except in cases of operational necessity, personal data should not be removed from University premises, or stored or processed on laptops or other portable devices.

It may sometimes be necessary to send records concerning individuals to people outside the University (for example, when the Chairman of a University committee is asked to take Chairman's action in respect of a student or member of staff and may retain his own record of that decision and copies of relevant papers). These people should be requested to return the papers concerned once the matter has been resolved, or to destroy them in an appropriate way, for example, by shredding.

All staff, students and other non-University employees who are authorised to have access to personal information, whether computerised or paper based, must be suitably trained and aware of the requirements imposed by the DPA, especially those relating to security. They must know what they need to do to ensure the University's compliance, and what the consequences may be for the University and for them personally if they do not follow procedures. The University provides regular in-house training sessions on records management, including data protection requirements, and general guidance on data protection is available on the University's website and Intranet.

The University cannot sidestep its obligations simply by outsourcing its data processing or data handling tasks to an outside body. If data held by the University are processed on its behalf by an external person or body (termed a 'data processor' in the Act), the University must be satisfied that the data processor is reliable and responsible and can give guarantees in respect of its security measures. The University itself must take steps to ensure compliance with those measures. The University must also enter into a formal written contract with the data processor requiring it to act only on instructions from the University and to comply with the obligations set out under the seventh principle. Arrangements with all suppliers who may have access to personal information held by the University should be reviewed annually.

Special care must be taken when disposing of computing equipment which is no longer required by the University. Before such equipment is sold or removed from University premises, all personal data in the memory of the equipment must be permanently removed. It is recommended that the equipment should be **double checked** to ensure that this has been done, and that a written record be retained for audit purposes.

9. The Eighth Principle: Exporting of data

This principle states that data shall not be transferred to a country outside the European Economic Area (that is the EU together with Iceland, Liechtenstein and Norway) unless that country has adequate data protection rights.

The principle does not apply where *inter alia* a data subject has given consent to the transfer, or where the transfer is necessary for the performance of a contract with the data subject or for taking steps, at the request of the data subject, with a view to entering such a contract. As with the first and second principles (see 5 above), the safest course for the University is to ensure that the data subject has given prior consent to any data transfer which falls within the scope of this principle.

Initial guidance from both the Information Commissioner and JISC was cautious on the subject of publication of personal data on the Internet, as it was thought that such publication might amount to a transfer of the data to a country outside the EEA, which would have been in contravention of this principle. However the decision in 2003 in the *Lindqvist* case made a distinction between the publication of data on a website, and the subsequent exportation of those

data to someone else outside the EEA who logged on to the website. This means that merely mounting the data on a website within the EEA does not in itself amount to exportation outside the EEA. But it does clearly facilitate such exportation and in itself constitutes processing for the purposes of the Act.

10. Exemptions

There are a number of exemptions in the Act which permit data controllers to process data in ways which are not normally permitted under the data protection principles, where this can be justified on public interest grounds. For example, the University as a data controller may be required to divulge personal data to the police or other authorities where the information is required in connection with matters such as the prevention or detection of crime or the assessment or collection of tax, or where disclosure is required by law or is necessary in connection with legal proceedings. The University will only make disclosures of this kind on receiving a certificate from the authority seeking the information to the effect it falls within a relevant exemption under the Act.

The processing of personal data may also be permitted where this is necessary for the legitimate interests of the data controller or the third party seeking the information, and does not at the same time prejudice the legitimate interests of the data subject. In a case involving a former student at another university who was falsely claiming a qualification he did not have, the Information Commissioner took the view that the university concerned would not be in breach of the Act if it were to disclose to the former student's parent that he had no qualification from the university. In this case, the former student was deemed to have no legitimate interests which could be prejudiced by this disclosure, and had no legal right to claim a qualification he had not been awarded; the university and the parent (who had been funding the supposed 'study') did have legitimate interests, and therefore disclosure could be made.

Any requests from outside authorities such as the police or the courts for the disclosure of personal data should be referred to the Data Protection Officer.

11. Records Management

Particular attention should be given to the following points relating to record keeping and disposal:

- Contracts with staff and third parties, which may relate to external records storage, data back-up or the destruction of confidential waste, should ensure that **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 compliant control within the semi-current records centre 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 data protection. 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, then deleted from the personal mailbox; if such a system is not available then e-mail should not be used. 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.
- **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 the Records Management Procedures Manual Best Practice Procedure No. 5: *Data Protection Act 1998 – procedure for answering requests for information* (available on the University Intranet at: <https://intranet.london.ac.uk/911.html>).

12. Further Information

Any questions relating to the Data Protection Act or this guidance, and any requests for further information should be directed in the first instance to the Data Protection Officer (email: data.protection@london.ac.uk).

LCA/IB/5.iii.02
 Revised 4.i.05
 Revised 14.iii.07
 Revised 19.ix.07



APPENDIX 1

**UNIVERSITY OF LONDON
REQUEST FOR ACCESS TO PERSONAL DATA**

1. Details of person requesting the information

Full name:

Address:

Tel. No:

Fax No:

Email address:

2. Are you the data subject?

YES: If you are the data subject please supply evidence of your identity, i.e. driving licence, passport, national identity card or photo-pass, a recent letter or bill from a utility company as evidence of address, and a stamped addressed envelope for returning the document

(Please go to question 4)

NO: Are you acting on behalf of the data subject with their written authority? If so, that authority must be enclosed. If not, what other legal justification have you for obtaining access to the data?

(Note that appropriate identification as above must be provided also.)

(Please go to question 3)

3. Details of the data subject (if different from 1)

Full name:

Address:

Tel. No:

Fax No:

Email address:



4. Please describe the information you seek together with any other relevant information. This will help to identify the information you require. Please tick the category into which your enquiry falls:

- Academic marks or course work details
- Disciplinary records
- Health and medical matters
- Political, religious or trade union information
- Personal details e.g. name, address, date of birth
- Other

Detailed description of information required:

The University charges a fee of £10 for each application. Cheques should be made payable to the University of London.

DECLARATION. To be completed by all applicants. Please note that any attempt to mislead may result in prosecution

I certify that the information given on this application form to the University of London is true. I understand that it is necessary for the University of London to confirm my/the data subject's identity and it may be necessary to obtain more detailed information in order to locate the correct personal data

Signature:

Date:

Note. The period of 40 days in which the University of London must respond to the request will not begin until it is satisfied on these matters and the fee of £10.00 has been paid.

Please return the completed form to the Data Protection Officer, University of London, Stewart House, 32 Russell Square, LONDON WC1B 5DN.

Documents which must accompany this application:

- evidence of your identity
- evidence of the data subject's identity (if different from above)
- authorisation from the data subject to act on their behalf (if applicable)
- the fee of £10.00
- stamped addressed envelope for return of proof of identity/authority documents