



Data Protection Policy

London Business School is committed to responsible data processing in accordance with its legal obligations as a registered data controller under the Data Protection Act 1998 ("the Act") and associated codes of practice issued by the Information Commissioner. The Act enhances the rights of individuals (including students, staff and any other individuals associated with the School) in respect of information held about them by the School. Staff owe a duty of care to the School when processing data about students, other employees or other individuals and advice from line managers should always be sought in any case of uncertainty.

London Business School takes the privacy and security of its staff members' and students' data seriously. The aim of this data protection policy is to ensure that all individuals about whom the School processes data are properly informed about the effect of the Act in respect of both their rights and their obligations.

1. IMPORTANT DEFINITIONS FROM THE ACT

"Personal Data"	means, broadly speaking, any information or data relating to an identifiable living individual. The Act now extends (with certain exceptions) to paper-based filing systems and other non-electronic collections of data as well as computer-based databases
"Data Subject"	means an individual about whom London Business School processes Personal Data
"Processing of Personal Data"	means almost any action involving Personal Data, including: obtaining; recording; holding; consulting; using; altering; disclosing and destroying such Personal Data
"Sensitive Personal Data"	means any data concerning a Data Subject's race or ethnic origin; political opinions; religious beliefs; trade union membership; physical or mental health; sexual life or criminal record. Additional rules apply under the Act to processing of Sensitive Personal Data
"Data Controller"	means London Business School when processing data about Data Subjects
"Data Processor"	means an external person or organisation (not being a member of staff at London Business School) who processes Personal Data on behalf of London Business School

2. WHAT SORT OF DATA DOES LONDON BUSINESS SCHOOL HOLD AND HOW DOES IT OBTAIN IT?

Generally, London Business School receives information about individuals from one or more of the following sources:

- directly from individuals themselves, for example when potential employees or students apply for a position with London Business School or to join a programme or subsequently during the course of that employment or that programme. This may include data such as name, address, date of birth, telephone number, career or educational history, health record, bank account details;
- from third parties, for example, by means of a reference from previous employers or academics;
- from third parties or individuals themselves in connection with the marketing and promotion of the School and its courses;
- occasionally from individuals' legal and/or financial representatives.

3. FOR WHAT PURPOSES DOES LONDON BUSINESS SCHOOL USE THIS DATA?

London Business School uses this data for a number of purposes, examples of which are outlined below:

- to administer and maintain staff records for the purposes of fulfilling the contract of employment (eg running the payroll);
- to administer and maintain student records for the purposes of student selection; providing educational services; career services; student association services; alumni services (including fundraising and directory publication);
- to maintain such records as may be required by legislation (eg health and safety and employment legislation);
- to respond to any query that individuals may raise with London Business School about matters relating to their employment, their education or any other matter;
- to disclose information about staff and former staff members or students and former students to future employers for reference purposes;
- to keep staff and former staff members informed (by post, telephone or e-mail) about matters relating to their employment or pension;
- to keep students and alumni informed (by post, telephone or e-mail) about relevant matters relating to London Business School;
- to use information about staff and students for the purposes of management planning and forecasting, research and statistical analysis;
- to disclose information to other companies and organisations associated with London Business School, including overseas associated companies and organisations, where appropriate;

- to market and promote the School and its courses worldwide;
- to disclose information about individuals in response to legislative/court orders.

4. CARING FOR INDIVIDUALS' DATA

London Business School owes certain obligations to individuals about whom it processes Personal Data, and such individuals have certain rights in relation to that data. Similarly, individuals employed by the School or students may at some stage be involved in processing Personal Data about other staff members, students or other individuals and in doing so they must be aware of their responsibilities to the School in carrying out any such processing.

The Act requires London Business School to adhere to certain standards relating to the gathering, use and disclosure of Personal Data. These standards are set out in the following 'Data Protection Principles'. A breach of one of these Principles could ultimately result in London Business School being prohibited from processing data. All individuals at London Business School involved in any way in the Processing of Personal Data relating to staff, students or others, must be aware of the Data Protection Principles.

London Business School will not divulge personal data to third parties without the consent of the individual concerned, except in connection with the purposes listed in Section 3 above, where the School may transfer or disclose personal data to third parties worldwide to perform specific services. All such third parties are prohibited from using this personal data except to provide these services to the School and they are required to maintain the confidentiality of the data.

The Data Protection Principles

- Personal Data must be obtained and processed fairly and lawfully.

Processing will only be fair and lawful where one of certain statutory preconditions is satisfied, the most obvious of which is where a Data Subject has given consent to such processing or where processing is necessary for performance of a contract with the Data Subject. In the absence of consent, processing will also be fair and lawful where it is (a) in the legitimate interests of the School and (b) it does not unduly prejudice the Data Subject's rights or interests.

More restrictive provisions apply to the processing of "Sensitive Personal Data" (principally the need to obtain explicit consent to processing). In any case of uncertainty as to the fairness or lawfulness of processing, further advice should be sought.

- Personal Data shall be held only for one or more specified and lawful purposes.

These purposes are disclosed by the School to the Information Commissioner and are publicly available. A copy may be obtained on request. Those processing data at the School should ensure that where consent is obtained for processing, Data Subjects are told of the purposes for which the data will be used.

- Personal Data held for any purpose or purposes shall not be used or disclosed in any manner incompatible with that purpose or those purposes.

Data cannot be used any differently from the registered purpose or disclosed to a party other than those notified to the Information Commissioner.

- Personal Data held for any purpose shall be adequate, relevant and not excessive in relation to the purpose or those purposes.

Data processed should only be that necessary to achieve the specified purpose.

- Personal Data shall be accurate and, where necessary, kept up-to-date.

Data is considered inaccurate if it is incorrect or misleading as to any matter or fact. Periodic reviews of databases should be carried out and databases must be amended when changes to data are made known to the School.

- Personal Data held for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

Redundant or out-of-date information should be deleted. Further guidance is available on request.

- An individual shall be entitled, at reasonable intervals and without undue delay or expense, to be informed by the Data Controller whether it holds Personal Data of which that individual is the subject; and to have access to any such data held by a Data Controller; and where appropriate, to have such data corrected or erased.
- Personal Data must be kept secure.

Appropriate security measures must be taken against unauthorised access, alteration, disclosure or destruction of Personal Data, and against accidental loss or destruction of Personal Data.

Factors involved when considering whether security measures are appropriate would include the nature of the Personal Data and the potential harm which could result from unauthorised access. It is necessary to consider the place where data is stored both in hard copy and electronically, access to filing cabinets, screens and other computer equipment and back-up procedures. Control over computer passwords is an important aspect of data security and passwords should not be disclosed to others within or outside London Business School.

- Personal Data should not be transferred outside the European Economic Area ("EEA") unless the country concerned provides an adequate level of protection for Data Subjects.

Care should be taken to ensure that Personal Data transferred outside the EEA will be processed by the recipient in accordance with the Data Protection Principles. The Data Subject should be asked to consent to such a transfer and be made aware that his/her personal data may be held under less stringent data protection laws as a consequence. Further advice should be sought in any case of uncertainty.

If any individual is unclear of his/her obligations in processing Personal Data under the Data Protection Act, he/she should contact Richard Frost, Associate Director, Office of the Deputy Dean and Secretary at the earliest opportunity.

London Business School will endeavour at all times (i) to adhere to the Data Protection Principles; (ii) to ensure Data Subjects are made aware of their rights

under the Act and (iii) to process data in accordance with the provisions of the Act.

5. RIGHTS OF DATA SUBJECTS

Data Subjects have certain rights under the Act in relation to the information which London Business School holds about them. These rights are set out below:

- Access to Personal Data (Subject Access). An individual may request in writing that London Business School discloses details of data which it holds about him/her and the purpose(s) for which such data are held. There is a standard form - a 'Subject Access Request Form' - that will be supplied on request and which must be returned with the relevant fee (£10) before a Subject Access application will be considered. London Business School will provide the information sought, in a permanent form, as at the time of the request, subject to any routine processing continuing between that time and the time of response and subject to any legal exemptions from disclosure. Subject Access requests will be met within 40 days of receiving the standard form and fee.
- An individual is entitled, by notice in writing, to require London Business School to cease (or not to begin) processing Personal Data on the grounds that it is causing, or is likely to cause, him/her or another substantial damage or distress and that damage or distress is or would be unwarranted. This does not apply where an individual has consented to the processing; the processing is necessary for entering into, or for the performance of, a contract with the individual; the processing is necessary for compliance with a legal obligation, to protect an individual's vital interests or to pursue the legitimate interests of London Business School's business unless prejudicial to the interests of the individual.
- An individual is entitled, by notice in writing, to require London Business School to ensure that no decision taken by or on behalf of London Business School which significantly affects him/her is based solely on the automated processing of their information, for the purpose of evaluating such matters as, for example, job applications or promotion. Individuals are also entitled to require London Business School to cease using Personal Data for the purposes of direct marketing.

6. TELEPHONE, E-MAIL AND INTERNET USAGE AND CCTV MONITORING

Any use of the Network at London Business School is subject to the current Terms and Conditions for the use of the London Business School Network. All CCTV use at London Business School is subject to the London Business School CCTV Recording Standard Code of Practice. Copies of both are available on request.

London Business School shall comply with all statutory requirements with regard to its obligations as the controller of a computer network, including the provisions of the Data Protection Act 1998; the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and any other relevant legislation that may apply from time to time.

London Business School shall not undertake any form of unnecessary e-mail, internet or other communication monitoring. Where monitoring is necessary this shall be carried out only in accordance with the relevant statutory provisions and in accordance with the current Terms and Conditions for use of the London Business School Network.

Principally, this means that London Business School shall only:

- carry out monitoring to prevent or detect crime; to investigate or detect unauthorised use of the Network or use in any way contrary to the Terms and Conditions for use of the Network or to ensure the effective operation of the Network (for example to detect viruses);
- carry out monitoring by way of spot checks rather than engaging in any form of continuous monitoring unless by way of an investigation into suspected misuse of the Network;
- monitor as far as possible by automated means to reduce the extent of information available to any person other than the parties to a communication;
- target any monitoring to areas of known risk, rather than any form of widespread monitoring;
- monitor where known misuse poses a significant threat to business efficiency;
- monitor without viewing the content of e-mail communications clearly marked as personal and London Business School shall notify staff when access to staff e-mails by other staff members may occur in their absence from work;
- carry out monitoring for any other reasonably justified purpose.

7. CONTACT DETAILS

For further information relating to the processing of data by London Business School, please contact:

Richard Frost
 Secretary and Planning Director
 London Business School
 Regent's Park
 London NW1 4SA

Telephone: 020 7000 7024
 Email: rfrost@london.edu

8. THE INFORMATION COMMISSIONER

For further information about individuals' rights in respect of the protection of personal data, please contact: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

or telephone 01625 545700 or fax 01625 524 510

Homepage: <http://www.informationcommissioner.gov.uk/>

=
 Revised – November 2006