Birkbeck
UNIVERSITY OF LONDON

Data Protection Policy and Code of Practice

DATA PROTECTION POLICY
and Code of Practice

Contents

DATA PROTECTION POLICY

Data Protection Policy
Birkbeck, University of London

1. **Introduction**
Birkbeck College needs to keep certain information about its employees, students and other users to allow it to monitor performance, achievements, and health and safety, for example. It is also necessary to process information so that the College can comply with its legal obligations and staff can be recruited and paid and courses organised. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

2. **To do this, Birkbeck College must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the 1998 Act).**

3. **In summary these state that personal data shall:**

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for that purpose.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights.
- Be kept safe from unauthorised access, accidental loss or destruction.
- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

4. **Birkbeck College and all staff or others who process or use personal information must ensure that they follow these principles at all times.**

5. **In order to ensure that this happens, the College has developed this Data Protection Policy and the accompanying Data Protection Code of Practice.**

6. **Status of this Policy**
This policy does not form part of the formal contract of employment for staff, or the formal offer of a place for study for students, but it is a condition of employment or study that employees and students will abide by the rules and policies made by the College from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

7. **The Data Controller and the Designated Data Controllers**
The College as a body corporate is the Data Controller under the 1998 Act, and the Governors are therefore ultimately responsible for implementation. However, the Designated Data Controllers will deal with day-to-day matters.

8. The College has three Designated Data Controllers. They are the Registrar, the Director of Human Resources, and the College Secretary.

9. Any member of staff, student, applicant or other individual who considers that the Policy has not been followed in respect of personal data about himself or herself should raise the matter with the appropriate Designated Data Controller, who would be:

For students: The Registrar

For staff: The Director of Human Resources

For all others: The College Secretary

10. The academic Schools and administrative Sections will themselves have designated staff who will provide the Registrar, the Director of Human Resources and the College Secretary with details of the data held in their academic School or administrative Section.

DATA PROTECTION POLICY

11. Responsibilities of Staff

All staff are responsible for:

- Checking that any information that they provide to the College in connection with their employment is accurate and up to date.
- Informing the College of any changes to information that they have provided, e.g. changes of address, either at the time of appointment or subsequently. The College cannot be held responsible for any errors unless the staff member has informed the College of such changes.

12. If and when, as part of their responsibilities, staff collect information about other people (e.g. about a student's course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff set out in paragraphs 10–13 of the College's Data Protection Code of Practice.

13. Student Obligations
Students must ensure that all personal data provided to the College is accurate and up to date. They must ensure that changes of address etc. are notified to the Registry.

14. Students who may from time to time process personal data as part of their studies must notify their supervisor/tutor, who should inform the Registrar, and must comply with the guidelines for data collection and security as set out in paragraphs 10–26 of the College's Data Protection Code of Practice.

15. Data Security
All staff are responsible for ensuring that:

- Any personal data that they hold is kept securely.
- Personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

16. *Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.*

17. Personal information should:

- Be kept in a locked filing cabinet, drawer, or safe;
  or
- If it is computerised, be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up;
  and
- If a copy is kept on a diskette or other removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

18. Further information on data security is given in paragraphs 14–26 of the College's Data Protection Code of Practice.

19. Rights to Access Information
All staff, students and other users are entitled to:

- Know what information the College holds and processes about them and why.
- Know how to gain access to it.
- Know how to keep it up to date.
- Know what the College is doing to comply with its obligations under the 1998 Act.

20. This Policy document and the College's Data Protection Code of Practice address in particular the last three points above. To address the first point, the College will, upon request, provide all staff and students and other relevant users with a statement regarding the personal data held about them. This will state all the types of data the College holds and processes about them, and the reasons for which they are processed.

21. All staff, students and other users have a right under the 1998 Act to access certain personal data being kept about them either on computer or in certain files. Any person who wishes to exercise this right should complete the Subject Access Request Form and submit it to the appropriate Designated Data Controller (see above).

22. The College will make a charge of £10 on each occasion that access is requested, although the College has discretion to waive this.

DATA PROTECTION POLICY

23. The College aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days, as required by the 1998 Act.

24. **Examination Marks**
During the course of their studies, students will routinely be provided with information about their marks for both coursework and examinations. However, exam scripts themselves are exempted from the subject access rules and copies will not ordinarily be given to a student who makes a subject access request. Further details are given in paragraph 38 of the College's Data Protection Code of Practice.

25. **Subject Consent**
In many cases, the College can only process personal data with the consent of the individual. In some cases, if the data is sensitive, as defined in the 1998 Act, express consent must be obtained. Agreement to the College processing some specified classes of personal data is a condition of acceptance of a student onto any course, and a condition of employment for staff. This includes information about previous criminal convictions.

26. Some jobs or courses will bring the applicants into contact with children, including young people between the ages of 16 and 18. The College has a duty under the Children Act 1989 and other enactments to ensure that staff are suitable for the job, and students for the courses offered. The College also has a duty of care to all staff and students and must therefore make sure that employees and those who use College facilities do not pose a threat or danger to other users.

27. The College may also ask for information about particular health needs, such as allergies to particular forms of medication, or any medical condition such as asthma or diabetes. The College will only use this information in the protection of the health and safety of the individual, but will need consent to process this data in the event of a medical emergency, for example.

28. Therefore, the application forms that all prospective staff and students are required to complete will include a section requiring consent to process the applicant's personal data. A refusal to sign such a form will prevent the application from being processed.

29. **Processing Sensitive Information**
Sometimes it is necessary to process information about a person's health, criminal convictions, race, and trade union membership. This may be to ensure that the College is a safe place for everyone, or to operate other College policies, such as the sick pay policy or the equal opportunities policy. Because this information is considered sensitive under the 1998 Act, staff (and students where appropriate) will be asked to give their express consent for the College to process this data. An offer of employment or a course place may be withdrawn if an individual refuses to consent to this without good reason. More information about this is available from the Designated Data Controllers.

30. **Publication of College Information**
The names of Senior Officers and Governors of the College or any other personal data relating to employees or Governors will be published in the annual Calendar and on the public Web site when any statute or law requires such data to be made public.

31. Certain items of information relating to College staff will be made available via searchable directories on the public Web site, in order to meet the legitimate needs of researchers, visitors and enquirers seeking to make contact with appropriate staff. Paragraphs 27–30 of the College's Data Protection Code of Practice set out the details of this scheme.

32. Individual Schools, Research Centres and Administrative Departments within the College may make additional staff or research student biographical details or other personal data available on their public Web sites. It may also be the case that students enrolled on certain courses may produce Web-based material containing personal data as part of their course work. All such activities are set out in detail in paragraphs 27–31 of the College's Data Protection Code of Practice.

DATA PROTECTION POLICY

33. Retention of Data

The College has a duty to retain some staff and student personal data for a period of time following their departure from the College, mainly for legal reasons, but also for other purposes such as being able to provide references and academic transcripts, or for financial reasons, for example relating to pensions and taxation. Different categories of data will be retained for different periods of time. The exact details of retention periods and purposes are set out on pages 11–12 of the College's Data Protection Code of Practice.

34. Conclusion

Compliance with the 1998 Act is the responsibility of all members of the College. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or to access to College facilities being withdrawn, or even to a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the appropriate Designated Data Controller.

DATA PROTECTION CODE of practice

Data Protection Code of Practice Birkbeck, University of London

1. Introduction

This Code of Practice must be read in conjunction with the College's Data Protection Policy document to give the fullest picture of Birkbeck's data protection regime. This document gives an introduction to some basic points of practice relating to the handling and processing of personal data at Birkbeck. It also lists the particular activities carried out within the College's administrative and academic departments that involve the handling and processing of personal data.[1]

2. Key Concepts

The Data Protection Act 1998 places an obligation upon Birkbeck, as a data controller, to collect and use personal data in a responsible and accountable fashion. Birkbeck College is committed to ensuring that every current employee and registered student complies with this Act to ensure the confidentiality of any personal data held by the College in whatever medium. Three key concepts to be considered are those of purpose, fairness and transparency.

3. Purpose

Data controllers can only process personal data where they have a clear purpose for doing so, and then only as necessitated by that purpose. Paragraphs 39–50 of this Code of Practice summarise the purposes for which the College processes personal data. Personal data cannot be processed for purposes that have not been defined and declared in the College's Data Protection Register entry (see paragraph 6 below).

4. Fairness

In defining the purposes for which Birkbeck processes personal data, the fairness of that processing must be considered. For some types of processing the required elements of fairness and legality are clearly outlined in the legislation, but for many others they are not. In such cases, Birkbeck has tried to take a broad approach to deciding what is fair in each case, based on an interpretation of the 1998 Act and in conjunction with advice from the Information Commissioner, the College's own legal advisors, and on wider practice within the UK HE sector.

5. Transparency

Members of staff, students and others must be able to feel that there is no intention to hide from them details of how their personal data are collected, used and distributed by the College. One of the functions of this Code of Practice is to provide that assurance.

6. Existing Notifications

The Act requires many data controllers to notify the Information Commissioner of the purposes for which personal data are processed, together with certain details of that processing. Those notifications are then held on a public register. The College has two existing Register entries – for the College and the Students' Union – that can be examined on-line at the following Web address: http://www.dpr.gov.uk/.

7. It is an offence for the College to hold personal data that falls outside of the classes declared in these notifications or to process personal data for any purposes that are not defined there. It is therefore very important that those who work with personal data in the course of their College duties are familiar with the details contained in these notifications.

8. Any changes that may be required should be passed to the College Secretary's Office as these entries are periodically reviewed and amended as necessary by the College Secretary.

9. Paragraph 35 of this Code of Practice gives details of the College's Designated Data Controllers, who are responsible for handling subject access requests and dealing with data protection enquiries within the College.

1. The wording of this document draws heavily on version 2.0 of the 'JISC Data Protection Code of Practice for the HE and FE Sectors', produced by Andrew Charlesworth, Senior Lecturer in IT Law at the University of Hull Law School.

The JISC document can be viewed on-line at: http://www.jisc.ac.uk/index.cfm?name=pub_dpacop_0101

DATA PROTECTION CODE of practice

Collection and Amendment of Personal Data

10. Collection of personal data

In most cases, the personal data held by the College will be obtained directly from the data subjects themselves. The law stipulates that a data protection notice must accompany any request for personal data. Any members of staff responsible for managing the collection of personal data for the legitimate activities of the College must ensure that a notice containing the following information is included in the request for that data:

- A statement that Birkbeck, University of London is the data controller
- The name and or job title of the specific member of staff responsible for the administration of the personal data being collected, to enable, for example, subsequent amendments to be submitted by the data subject
- A clear explanation of the types of data being collected and the purposes for which that data will be processed
- Any further information that is considered necessary to ensure that the data processing can be described as being fair, for example details of any third parties to whom the data might be disclosed
- A statement making it clear that by submitting the personal data, the data subjects are giving their consent for the processing of the data for the stated purposes to take place.

11. Amendment of personal data

From time to time data subjects will wish to update some of their personal data held by the College, for example their home addresses or other contact details previously submitted. To do this, the data subjects must either contact the specific member of staff designated in the data protection notice at the time the data was submitted, or the appropriate Designated Data Controller as set out in paragraph 35. Proof of identity will be required before any amendments can be made.

12. As and when 'self-service' computer-based administrative systems are introduced for staff, students or others, the data subjects themselves will be able to take responsibility for the maintenance of certain elements of their personal records.

13. These systems will incorporate the necessary authentication and security mechanisms to ensure that data subjects are only able to view and amend their own data.

14. Security of personal data

Of fundamental importance within any data protection regime is the security of the personal data that is being processed. Data subjects have the right to expect that their personal data will be kept and processed securely and that no unauthorised disclosures or transfers will take place to anyone either within or outside the College. Authorised disclosures or transfers are those that are defined within the appropriate Notifications (see paragraphs 6–9 above) and declared to the data subject either at the point of data collection or subsequently, the necessary consent for disclosure or transfer having been obtained if required.

15. To help ensure the security of personal data within the College, all those in Birkbeck who process such data in the course of performing their duties are required to follow the general guidelines set out below.

16. Secure storage of personal data

Each member of staff whose work involves storing personal data, whether in electronic or paper format, must take personal responsibility for its secure storage, in line with Birkbeck's Data Protection Policy, which states that personal data should:

- Be kept in a locked filing cabinet, drawer, or safe;
  or
- If it is computerised, be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up;
  and
- If a copy is kept on a diskette or other removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

DATA PROTECTION CODE of practice

17. Ordinarily, personal data should never be stored at staff members' homes, whether in manual or electronic form, on laptop computers or other personal portable devices or at other remote sites.

18. Staff should be aware that log files would record details of all users who access, alter or delete or attempt to access, alter or delete centrally held computerised databases and files containing personal data.

19. **Secure processing of personal data**
While staff members in the course of performing their legitimate duties are using personal data, reasonable precautions must be taken to ensure the safety and privacy of that data. For example:

- In open-plan offices, computer screens that could potentially be displaying personal data should not be positioned such that unauthorised staff may readily see that data, and password-protected screensavers should be used.
- Personal data in manual form, such as in paper files, correspondence or database printouts, should not be left in view in open-plan offices while the relevant staff members are away from their desks. They should instead be locked away or at least covered.
- Where manual records containing personal data are accessible to a number of staff in the course of their legitimate activities, access logbooks should be used where practicable to help monitor the whereabouts and use of such records.

20. Ordinarily, personal data should not be processed at staff members' homes, whether in manual or electronic form, on laptop computers or other personal portable devices or at other remote sites. In cases where such off-site processing is felt to be necessary or appropriate, the agreement of the relevant Head of School or Department must be obtained, and all the security guidelines given in this document must still be followed.

The disclosure and transfer of personal data

21. **Authorised and unauthorised disclosures**
Staff members working with personal data will be made aware by their line managers or other appropriate staff of the purposes for which the data is processed and the legitimate parties either within or outside Birkbeck to whom that data, either in whole or in part, may be disclosed or transferred. Personal information must not be disclosed either orally or in writing or via Web pages or by any other means, manual or electronic, accidentally or otherwise, to any unauthorised third party.

22. *Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.*

23. **Security of data during transfer**
Where personal data is transferred between staff members within the College in the course of their legitimate activities, the level of security appropriate to the type of data and anticipated risks should be applied. For example, sensitive personal data should either be transferred by internal mail in sealed envelopes or by hand. If transferred by e-mail, such data should normally either be encrypted or sent in a password-protected attachment (for example using Microsoft Word's 'require password to open' feature), with the password being supplied separately. Further advice on secure email and password protection can be obtained from Central Computing Services.

24. **Disclosures outside the College**
When a request to disclose or amend personal data relating to a member of the College (student or staff) is received from an individual or organisation outside the College, in general no data should be disclosed or amended unless the authority and authenticity of the request can be established. Disclosures requested by those claiming to be relatives or friends should be refused unless the consent of the data subject is obtained for such disclosures or in one of the few situations where disclosure without consent is permitted by the law (see: http://www.jisc.ac.uk/index.cfm?name=pub_dpacop_0101#683 for further information).

25. Requests for the disclosure of personal data from the Police, Government bodies, the British Council or other official bodies and agencies should be investigated sufficiently to verify the authenticity of the request and may then be acted upon if there is a legal requirement for such disclosure or the consent of the data subject has been given for the disclosure.

26. Details of any specific procedures and practices to be adopted when responding to requests for disclosure in individual administrative Departments or Academic Schools within the College will be available from the appropriate senior members of staff.

Publication of College Information

27. While the majority of personal data held by the College is processed for internal administrative purposes and is never disclosed outside the institution, some categories of data are routinely or from time to time released through one or more forms of publication.

28. **Legal obligations**
When required by law or College statute, the names of Senior Officers and Governors of the College and certain other personal data relating to employees and Governors are published in the annual Calendar and on the Web site. The College also fulfils all obligations placed upon it by its relationship with various funding bodies, Government Agencies and the like with regard to the release of personal data and statistical information concerning students and staff. Data subjects are informed of the College's obligations in this respect at the time the data is collected.

29. **Staff Directory**
In order to meet the legitimate needs of researchers, visitors and enquirers to be able to make contact with appropriate staff, Birkbeck intends to make available on its public Web site a directory containing the job title, organisational unit, title, forename, surname, office telephone number, office room number and location and office e-mail address of each staff member. However, at the time of appointment and at any time while in post (via a request to the designated Data Controller) each individual member of staff will be able to specify the level of detail that will appear in this public directory, i.e. being able to request that the following be omitted: title, forename, e-mail address.

The Web-based public directory will be searchable by name and organisational unit and will only return personal contact data for those staff that have given their consent for this disclosure. A complete directory is available on the College intranet, but this is password-protected and is only available to current students and staff. A printed directory is made available to all members of staff within the College, but is not ordinarily given to anyone else.

30. **Staff personal data on Web pages**
Apart from the staff directory described above, staff biographical details or other personal data may be published on Birkbeck's Web sites or in other media, but only where the staff concerned have given their consent for such information to be made publicly available. However, publication in this way does not mean that such data have been placed into the public domain. Birkbeck retains control and copyright of such data, and the data must not be reproduced or further processed without the College's express permission.

31. **Student personal data on Web pages**
Apart from the obligations mentioned above (paragraph 28) the College will not ordinarily reveal any personal details of students enrolled at Birkbeck to any individual or body outside the College. However, some research students may consent to contact details or other personal data being published, for example via the College's public Web sites. It may also be the case that students enrolled on certain courses may produce Web-based material containing personal data as part of their course work. In such cases, responsibility for such disclosures rests entirely with the individual students concerned and is not indicative of any College-wide policy.

Retention and Disposal of Personal Data

32. The retention of personal data

The College has a duty to retain some staff and student personal data for a period of time following their departure from the College, mainly for legal reasons, but also for other purposes such as being able to provide references and academic transcripts, or for financial reasons, for example relating to pensions and taxation. Some material will also be retained to form part of the official College archive (selected following the guidance given in the JISC publication '*Study of the Records Life Cycle*', available at http://www.jisc.ac.uk/index.cfm?name=recordsman_papers_cycle). Different categories of data will be retained for different periods of time, and these are set out in the table overleaf.

33. The disposal of personal data

When a record containing personal data is to be disposed of, the following procedures will be followed:

- All paper or microfilm documentation containing personal data will be permanently destroyed by shredding or incinerating, depending on the sensitivity of the personal data.
- All computer equipment or media that are to be sold or scrapped will have had all personal data completely destroyed, by re-formatting, over-writing or degaussing.

34. Employees and, where appropriate, students, will be provided with guidance as to the correct mechanisms for disposal of different types of personal data and audits will be carried out to ensure that this guidance is adhered to. In particular, employees and students will be made aware that erasing/deleting electronic files does not equate to destroying them.

DATA PROTECTION CODE of practice

Minimum Retention Periods for Records Containing Personal Data

Type of Record	Minimum Retention Period	Reason for Length of Period
Personnel files including training records, notes of disciplinary and grievance hearings, and appraisal forms	6 years from the end of employment	References and potential litigation
	Certain personal data may be held in perpetuity	Selected material will form part of the official College Archive
Letters of reference	6 years from the end of employment, by the author of the reference letter	References and potential litigation
Application forms/interview notes	At least 6 months from the date of the interviews	Time limits on litigation
Facts relating to redundancies where fewer than 20 redundancies	6 years from the date of redundancy	As above
Facts relating to redundancies where 20 or more redundancies	12 years from the date of the redundancies	Limitation Act 1980
Income Tax and NI Returns, including correspondence with tax office	At least 3 years after the end of the financial year to which the records related	Income Tax (Employment) Regulations 1993
Statutory Maternity Pay records and calculations	As above	Statutory Maternity Pay (General) Regulations 1986
Statutory Sick Pay records and calculations	As above	Statutory Sick Pay (General) Regulations 1982
Wages and salary records	6 years	Taxes Management Act 1970
Accident books, and records and reports of accidents	3 years after the date of the last entry	Social Security (Claims and Payments) Regulations 1979; RIDDOR 1985
Health Records	During employment	Management of Health and Safety at Work Regulations
Health Records where reason for termination of employment is connected with health, including stress related illness	3 years	Limitation period for personal injury claims
Medical records kept by reason of the Control of Substances Hazardous to Health Regulations 1999	40 years	The control of Substances Hazardous to Health Regulations 1999
Ionising Radiation Records	At least 50 years after last entry	Ionising Radiations Regulations 1985
Applicant records for those who are rejected or who decline an offer	No more than 4 months after the start of the academic year	Permits institution to handle enquiries from the data subject
Student records of those not completing enrolment	Within one academic year	Permits institution to handle delayed enrolments
Student records, including enquiries, applications, admissions, assessment, awards, attendance and conduct	At least 6 years from the date that the student leaves the institution, in case of litigation for negligence	Limitation period for negligence
	At least 10 years for personal and academic references	Permits institution to provide references for a reasonable length of time
	Certain personal data may be held in perpetuity	While personal and academic references may become 'stale', some data e.g. transcripts of student marks may be required throughout the student's future career. Upon the death of the data subject, data relating to him/her ceases to be personal data. Some selected material will form part of the official College Archive.

Subject Access Requests

35. All staff, students, applicants and other users have a right under the Act to access certain personal data being kept about them at Birkbeck either on computer or in certain files. Any person who wishes to exercise this right should complete the Subject Access Request Form in Annexe 1 and submit it to the appropriate Designated Data Controller, who is:

For students: The Registrar

For staff: The Director of Human Resources

For all others: The College Secretary

36. The College will make a charge of £10 on each occasion that access is requested, although the College has discretion to waive this.

37. The College will comply with requests for access to personal information as quickly as is practicable, but will ensure that the information is provided within 40 days, as required by the Act.

38. Students and former students should be aware that exam scripts are exempted from the subject access rules and copies will not ordinarily be given to those who make a subject access request. However, a copy or summary of both internal and external examiner's comments can be requested as part of a subject access request. If such a request is made before the results of the examination are announced, the College will provide the information within 5 months of the request being received or 40 days from the announcement of the result, whichever is the earlier, as required by the Act.

The Processing of Personal Data within Specific Administrative Departments and Academic Schools

Activities involving the processing of personal data

39. Listed In the following sections are categories of activities carried out within each of the specified organisational units within the College that involve the processing of personal data. It is the responsibility of the appropriate Directors and Heads to ensure that sufficiently detailed guidance is given to their staff to enable them to carry out these activities in accordance with the requirements of the Data Protection Act 1998.

40. Faculties, Schools and Research Centres

Admissions administration

Enquiries administration

Events/conference administration

Faculty/School/Centre staff and function lists publication (e.g. on Web page)

Examination administration and marking

Marketing

Publication activities (including advertising and Web sites)

Research activities and administration

Staff management (includes performance, appraisal and development records, leave records, expenses records, etc)

Staff recruitment

Student assessment activities

Student records administration/student support

Supplier/order/invoice administration

Systems administration (e-mail, back-up/ storage, authentication, system logs, etc [in some cases])

Teaching activities and administration

Teaching performance/assessment/review activities

DATA PROTECTION CODE of practice

41. Central Computing Services

Department staff and function lists publication (e.g. on Web page)

Staff directory maintenance

Staff management (includes performance, appraisal and development records, leave records, expenses records, etc)

Staff recruitment

Student registration

Student and staff support activities and records/ RMS Service Desk

Supplier/order/invoice administration

Systems administration (MIS, e-mail, back-up/ storage, authentication, system logs, etc)

Telephone system administration

Training records administration (inc. ECDL and WebCT)

Web site forms (although usually created for another Department)

Workstation room bookings administration

42. College Secretary's Office

Archives management

Corporate planning and management activities

Data protection SAR administration

Department staff and function lists publication (e.g. on Web page)

Governance activities (Committees, maintenance of the Register of interests of Governors and senior administrative staff, etc)

Health and Safety activities and administration

Staff management (includes performance, appraisal and development records, leave records, expenses records, etc)

Staff recruitment

Supplier/order/invoice administration

43. Estates and Facilities

CCTV

Department staff and function lists publication (e.g. on Web page)

Estates and Facilities management and letting (inc. catering contracts, cleaning contracts, etc)

Help desk administration

Mail system administration

Security/access control systems and records

Staff management (includes performance, appraisal and development records, leave records, expenses records, etc)

Staff recruitment

Supplier/order/invoice administration

Telephone Operator activities

44. External Relations

Alumni relations management

Department staff and function lists publication (e.g. on Web page)

Events/conference administration

Fundraising activities/donor administration etc

Graduation ceremonies administration

Mailing list administration and use

Marketing

Market research

News/press release activities/public relations

Other publication activities

Staff management (includes performance, appraisal and development records, leave records, expenses records, etc)

Staff recruitment

Supplier/order/invoice administration

45. Finance

Archives management

Department staff and function lists publication (e.g. on Web page)

Financial management and accounting

Payroll administration

Pension scheme administration

Research grants administration and IPR administration

Staff management (includes performance, appraisal and development records, leave records, expenses records, etc)

Staff recruitment

Student financial records administration

Supplier/order/invoice administration

46. Human Resources and Staff Development

Archives management

Data protection SAR administration

Department staff and function lists publication (e.g. on Web page)

Employee relations management

Records or monitoring in accordance with the Race Relations Amendment Act 2000

Staff development and support activities/administration

Staff management (includes performance, appraisal and development records, leave records, expenses records, etc)

Staff records administration

Staff recruitment

Supplier/order/invoice administration

47. Library

Departmental staff and function list publication (eg. on Web page)

Loan and inter-library loan administration

Security/access control systems and records

Staff management (includes performance, appraisal and development records, leave records, expenses records, etc)

Staff recruitment

Staff and student support activities and records

Supplier/order/invoice administration

Systems administration (catalogue, back-up/ storage, authentication, system logs, etc)

48. Master's Office

Department staff and function lists publication (e.g. on Web page)

Staff management (includes performance, appraisal and development records, leave records, expenses records, etc)

Staff recruitment

Supplier/order/invoice administration

49. Registry

Admissions administration

Archives management

Assessment administration

Awards administration and conferment

Department staff and function lists publication (e.g. on Web page)

Data protection SAR administration

Enquiries administration

HESA returns activities

Staff management (includes performance, appraisal and development records, leave records, expenses records, etc)

Staff recruitment

Student disciplinary activities

Student records administration, including disability information

Student support activities

Supplier/order/invoice administration

Teaching performance/assessment/review activities

50. Students' Union

Clubs and Societies activities and administration

Publishing activities

Student records administration

Student support activities

Staff management (includes performance, appraisal and development records, leave records, expenses records, etc)

Staff recruitment

Supplier/order/invoice administration

Union officers/staff and function lists publication (e.g. on Web page)

51. Vice-Master's Office

Admissions administration

Archives management

Assessment administration

Awards administration and conferment

Business relations activities

Consultancy administration

Department staff and function lists publication (e.g. on Web page)

Enquiries administration

Events/conference administration

Faculty/School/Centre staff and function lists publication (e.g. on Web page)

Examinations administration and marking

Mailing list administration and use

Marketing

Market research

Publication activities (including advertising and web sites)

Staff management (includes performance, appraisal and development records, leave records, expense records etc.)

Staff recruitment

Student assessment activities

Student disciplinary activities

Student records administration, including disability information

Student support activities

Supplier/order/invoice administration

Teaching activities and administration

Teaching performance/assessment/review activities

Annexe 1
Birkbeck

Subject Access Request Form

Birkbeck UNIVERSITY OF LONDON

1. Details of the person requesting the information.

Full name: _____

Address: _____

_____

_____

_____

Telephone number: _____

Fax Number: _____

Email: _____

2. Are you the Data Subject?

☐ YES

If you are the Data Subject please supply evidence of your identity i.e. library card, driving licence, birth certificate (or photocopy) and, if necessary, a stamped addressed envelope for returning the document. Please also state your relationship to Birkbeck:

☐ I am a current/former member of staff

☐ I am a current/former student

☐ I am neither of the above

Please now go to question 5.

☐ NO

Are you acting on behalf of the Data Subject with their written authority? If so, that authority must be enclosed. Please also state the relationship of the Data Subject to Birkbeck:

☐ The Data Subject is a current/former member of staff

☐ The Data Subject is a current/former student

☐ The Data Subject is neither of the above

Please now go to questions 3 and 4.

3. Details of the Data Subject (if different from 1.)

Full name: _____

Address: _____

_____

_____

_____

Telephone number: _____

Fax Number: _____

Email: _____

4. Please describe your relationship with the Data Subject that leads you to make this request for information on their behalf.

_____

_____

_____

_____

_____

_____

5. If you wish to see only certain specific document(s), for example a particular examination report, a specific departmental file etc, please describe these below:

_____

_____

_____

_____

_____

_____

_____

6. If you would like a more general search, please note that the College is able to search the following sections for personal data. Please indicate the sections that you would like searched:

- ☐ Registry
- ☐ Human Resources
- ☐ Library
- ☐ Finance
- ☐ School/Faculty/Research Centre files and information systems

Please specify which School/Faculty/Research Centre(s):

_____

_____

_____

- ☐ Other
- ☐ Administrative Department files and information systems

Please specify which Administrative Department(s):

_____

_____

_____

_____

_____

7. Declaration

I, _____, certify that the information given on this application form is true. I understand that it is necessary for the College to confirm my/the Data Subject's Identity and it may be necessary for more detailed information to be obtained in order to locate the correct information.

Signed: _____

Date: _____

Please return the completed form to the appropriate Designated Data Controller at the address given below:

For students/ former students: The Registrar

For staff/former staff: The Director of Human Resources

For all others: The College Secretary

Birkbeck, University of London, Malet Street, Bloomsbury, London WC1E 7HX

Documents which must accompany this application are:

- evidence of your identity
- evidence of the Data Subject's identity (if different from above)
- evidence of the Data Subject's consent to disclose to a third party (if required as indicated above)
- a fee of £10 (cheques to be made payable to Birkbeck College)
- a stamped addressed envelope for return of proof of identity/authority documents, where appropriate

Please note that the College reserves the right to obscure or suppress information that relates to other third parties (under the terms of Section 7 of the Data Protection Act 1998).

Office use only

Request received: _____

Date completed: _____

Notes:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

This form is based, with grateful acknowledgement, on an example given on the Lancaster University Data Protection Project website at: http://www.dpa.lancs.ac.uk/approved/subject_access_requests.htm

Birkbeck, University of London
Malet Street, Bloomsbury
London WC1E 7HX
Tel 020 7631 6751
Fax 020 7631 6750
www.bbk.ac.uk

As London's leading provider of part-time university courses, Birkbeck offers a broad range of subjects at a variety of levels. For further details of our short courses, certificates, diplomas, undergraduate degrees, and postgraduate taught and research opportunities call 0845 601 0174.
For disability enquiries call 020 7631 6315.

This document is available in large format.
For details, call the Disability Office on 020 7631 6315.

July 2004