

## **Institute of Education, University of London**

### **Data Protection & Records Management Policy**

1. Policy statement & definitions
2. Data Protection
  - 2.1 Definition
  - 2.2 The eight principles of the Data Protection Act
  - 2.3 Sensitive personal data
  - 2.4 Requests for access to personal data
  - 2.5 Responsibilities and good practice
  - 2.6 Research data security
3. Records Management:
  - 3.1 Definition
  - 3.2 How does records management help?
  - 3.3 What does records management involve?
  - 3.4 Records management good practice
4. Further guidance & Information
  - 4.1 Related policies
  - 4.2 Your Records Manager
  - 4.3 The Bloomsbury Colleges Records Management Group
  - 4.4 Useful Links

#### **Appendices:**

- A. Subject Access Requests (SAR)
  - i. Guidance
  - ii. Proforma
  - iii. SAR request sheet
- B. Research Data Security Guidance
- C. Data Protection Register

## 1. Policy Statement

1.1 All IoE staff, students and visitors are expected to abide by the overarching principles and purposes laid out in this policy statement and provided in detail in the full Data Protection & Records Management policy of the Institute of Education of which this is a part.

1.2 The IoE is registered with the Information Commissioner's Office (ICO) as a data controller (see appendix 1. for a full copy of our register), and we gather, hold and process personal data for 11 stated purposes:

- i. Staff, Agent and Contractor Administration
- ii. Advertising, Marketing, Public Relations, General Advice Services
- iii. Accounts & Records
- iv. Education
- v. Student and Staff Support Services
- vi. Research
- vii. Other Commercial Services
- viii. Publication of the University Magazine
- ix. Crime Prevention and Prosecution of Offenders
- x. Alumni Relations
- xi. Crime Prevention and Prosecution of Offenders (CCTV)

1.3 All personal data is to be gathered, held, processed in accordance with legislation (the Data Protection Act 1998) and good practice (e.g. the Information Commissioners Office, JISC, Chartered Institute of Personnel and Development), and other relevant professional and ethical codes of conduct.

1.4 Deliberate abuse of the Data Protection principles by members of staff or students will be treated as gross misconduct and disciplinary action will be taken.

1.5 Definitions:

- "data controller": a data controller is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.
- "Staff", "students" and "other data subjects": may include past, present and potential members of those groups.
- "Other data subjects" and "third parties": may include contractors, suppliers, contacts, referees, friends or family members.
- "Processing": refers to any action involving personal information, including obtaining, viewing, copying, amending, adding, deleting, extracting, storing, disclosing or destroying information.

## **2. The Data Protection Act (1998)**

2.1 Data Protection provides a safeguard for personal privacy in relation to computerised or other systematically filed information. The Data Protection Act 1998 (DPA) regulates the use of **personal data**, meaning information about identifiable, living human beings.

### **2.2 The eight principles of the Data Protection Act are as follows:**

**First Principle** - "Personal data shall be processed fairly and lawfully"

**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 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 protections to the rights and freedoms of data subjects in relation to the processing of personal data"

**2.3 Sensitive personal data** includes ethnic origins, health, trade union membership, sexual life, and religious or political beliefs. There are stronger rules on the use of this data, and in general it can only be collected and processed with individuals' explicit consent. Advice should be sought from the IoE's Records Manager on the gathering, storage and processing of sensitive personal data.

**2.4 Requests for access to personal data (Subject Access Requests)** People whose data is kept (data subjects) have the right to be informed whether data on them is held and the purpose for which the information is used, and to obtain a copy of the information about them – this can be done by making a subject access request (Appendix A ). This right now applies to most types of information held about an individual in electronic or paper form, subject to certain exemptions. Data Protection requests have to be submitted in writing, and may involve proof of ID and payment of a statutory fee. A response has to be sent within 40 calendar days.

## **2.5 Responsibilities and Good Practice**

If you are responsible for the collection of personal data (either as a manager or supervisor or as an individual) then:

- be sure that data subjects have been informed about how the information will be used and who it will be shared with. This is called fair process notification and the notification should consist of the following information as a minimum:
  - Why the data needs to be gathered and how the data will be used;
  - Any third parties outside the IOE to whom the data will be disclosed or transferred;
  - The fact that completion of the form will be taken as consent by the data subject to the use of the data as outlined.
- take measures to ensure personal data is up to date, accurate, appropriate and secure. Electronic files should be password protected and access to computers or databases containing personal data should be timed out, hardcopy files should be kept in secure cabinets or draws in lockable rooms. Personal data should not be left out on desks when they are unattended.
- consider Data Protection before releasing data to third parties, especially those outside your institution. Remember that the family and friends of students and staff have no automatic right to data about them; nor do the police and the government, unless certain conditions are met. If in doubt about whether to release personal data, contact the Records manager;
- do not keep personal data for longer than is necessary and always dispose of personal data securely and thoroughly. Follow the records retention guidance for your department or use the JISC model retention schedule where a schedule has not yet been developed for your department;
- remember that people have the right to ask about data held on them. Requests for personal data should normally be referred to the IoE's Record Manager. Guidance on the procedure for making requests is contained in Appendix A.

## 2.6 Research Data Security

The gathering, storage and processing of data for the purposes of research has the potential to increase the variety of issues relating to consent, fair and lawful processing, transfer to third parties and security. These issues and recommended practices are detailed in Appendix B: Research Data Security Guidance.

## 3. Records management

3.1 Records management is about ensuring that the information which we need to document what we do is generated and kept as efficiently as possible. Records act as evidence of our decisions and activities, and preserve information which we may need in the future. In the past, records were kept in paper form, but today most records are generated and kept electronically. Our information is now subject to legislation which requires us to manage it effectively, to meet Data Protection requirements and so that we can produce information when it is requested under the Freedom of Information Act or the Environmental Information Regulations (see the Transparency and Freedom of Information Policy). However, the main reason for having good records management is that it helps us to work better.

### 3.2 How does records management help?

- **We can find the information we need, when we need it.** Records management helps us to organise our records in a consistent and coherent way, saving time in looking for information.
- **It saves space** (both physical storage space and server space), by reducing duplication and ensuring that records are kept for no longer than necessary. Records are disposed of according to agreed procedures.
- **Our records have value as evidence.** Records are kept in ways which ensure that their authenticity cannot be challenged, e.g. in a court of law.
- **It protects us and the Institution.** We will have the information which we need to defend our legal rights and those of others.
- **We will meet legal, regulatory and contractual requirements.** Good records management is not only necessary for Freedom of Information and Data Protection reasons. Regulatory bodies like the Quality Assurance Agency may require us to keep records, and we also need to keep records to show compliance with contracts and for audit purposes.

### 3.3 What does records management involve?

Records management focuses on creating two types of standards for staff to follow:

- **Classification schemes.** These provide a common way of organising your records, according to subjects or business functions and activities. They allow you to organise your records hierarchically, and can be applied to paper files, Windows folders and email folders. Records should also be classified in relation to how long they should be kept (see under retention schedules) and current usage requirements. The latter can be defined as follows:

**Current records:** are those needed for frequent processing or reference by the creating department. Current records are the responsibility of the creating faculty, unit or department. They must be filed and stored appropriately within meaningful record systems. If an activity ceases and the file is no longer needed for regular reference or processing, it should be closed and transferred from the current record keeping system.

**Semi-current records:** are those which are no longer processed or used regularly, but which need to be retained for a fixed period for reference, administrative or legal reasons. Semi-current records are the responsibility of the creating faculty, unit or department. They must be filed and stored appropriately within meaningful record systems

**Disposal:** records may be disposed of once their current and semi-current life has expired. Records must be disposed of according to agreed retentions schedules. Records must be disposed of in a manner appropriate to their confidentiality or sensitivity. Once a retention schedule is in place records that are no longer needed must be disposed of or transferred to the Archives.

**Archive:** records should be transferred to the Archive only once their current and semi-current life has expired. Records of long-term historical or evidential value must be transferred to the Archive and *not* stored in offices. Once records have been transferred to the Archive they cannot be recalled by faculty, units or departments for further filing or processing. They will be made available for reference.

- **Retention schedules.** These specify how long you should keep common types of records. A model classification scheme and retention schedule for higher education has been developed by the Joint Information Systems Committee (JISC). The JISC retention schedule is the recommended good practice for the sector and should be used as the default retention schedule across the Institute.

### **3.4 Records management: Good Practice**

- Use appropriate and professional language, particularly when referring to individuals. Remember that what you write could be released under Data Protection or Freedom of Information.
- Remember that records are owned by your institution. You can't take them with you when you leave, and you have a duty to keep them in an orderly state. Records management is much easier if you build it into your daily working practices.
- Follow any records management standards or procedures which have been developed in your Institution. Contact the IoE's Records Manager for advice.
- If you don't have them already...
  - a. Set up a classification scheme and retention schedule (contact the IoE's Records manager first). You can use the JISC standards as guidance (see above). Aim to use the same scheme for your paper and electronic information, so that your records are organised consistently.
  - b. Set up a naming convention for your electronic files. This will make it easier to identify what a file relates to, without having to open it.
- Remember that emails are records too! Most correspondence now takes place by email, and email is used to make key decisions. Make sure that relevant emails are saved into your record keeping system, e.g. by printing them out and adding them to paper files if you keep your records in paper form. Don't leave emails permanently in your in box or sent items folder.
- Use shared directories or shared paper files for information which your colleagues need to access. Leaving it in your personal files/directories makes it difficult for others to find what they need, e.g. when you are away. Set up a booking in/out system for paper files, so that you know where they are.

## **4. Further Guidance, Information & Support**

### **4.1 Related Policies**

1. Computer Security Policy
2. Email Etiquette
3. Misconduct in relation to Academic, Research and Scientific Activities:  
Code of Practice for enquiring into - ~
4. Transparency and Freedom of Information Policy

### **4.2 Your Records Manager:**

Matthew Grigson

Assistant Secretary

Directorate

Email: [recordsmanager@ioe.ac.uk](mailto:recordsmanager@ioe.ac.uk) or [m.grigson@ioe.ac.uk](mailto:m.grigson@ioe.ac.uk)

Telephone: 020 7612 6008

### **4.3 The Bloomsbury Colleges Records Management Group**

The Bloomsbury Colleges (<http://www.bloomsbury.ac.uk/>) is a consortium consisting of six University of London institutions. The BCRMG exists to promote co-operation among the Colleges in the areas of Data Protection, Freedom of Information and records management. Further information about the Group, including links to resources in each institution, is available at <http://www.soas.ac.uk/about/index.cfm?navid=2876>.

### **4.4 Useful Links:**

Information Commissioners Office: <http://www.ico.gov.uk/>

JISC Information Governance Gateway: <http://www.jigg.ac.uk/>

Policy Approval: 29.04.2008

Policy Review Date: 3 years: 29.04.2011

## **Guidance on making a request for access to personal data held by the Institute of Education**

### **1. What are your rights?**

The Data Protection Act 1998 gives individuals a right of access to the personal data which organizations hold about them, subject to certain exemptions (see 2. below).

Requests for access to personal data are known as **Subject Access Requests**. This page explains how to submit a subject access request to Institute of Education, how we will handle your request, and your right to complain if you are dissatisfied.

If you submit a subject access request to Institute of Education, you are entitled to be told whether we hold any data about you. If we do, you also have the right:

- To be given a description of the data, the purposes for which the data are being processed, and those to whom the data may have been disclosed;
- To be given a copy of the data in an intelligible form, with any unintelligible terms explained;
- To be provided with any information available to Institute of Education about the source of the data; and
- If you specifically request it, to be given an explanation as to how any automated decisions taken about you have been made.

These rights apply to electronic data, and to data in "manual" (i.e. non-electronic) formats, subject to certain limitations in regard to unstructured manual data (see 3. below). Further information about your rights under the Data Protection Act is available on the website of the Information Commissioner ([www.ico.gov.uk](http://www.ico.gov.uk)).

### **2. What are the exemptions?**

The Data Protection Act includes various exemptions which specify the circumstances in which an organization can refuse to provide access to personal data. The most likely situations in which Institute of Education could lawfully refuse a subject access request are where:

- The release of the data would jeopardise the prevention or detection of crime, or the apprehension or prosecution of offenders;
- You have requested access to an examination script, other than examiners' comments;
- You have requested data contained in a confidential reference provided by Institute of Education;
- You have requested data which record Institute of Education's intentions in relation to any negotiations with you, and the release of the data would prejudice the negotiations;
- The data is covered by legal professional privilege; or
- You have requested access to data which have been retained for the purposes of historical or statistical research, the conditions set out in the Data Protection Act

for processing for research purposes have been met, and the results of the research have not been published in a way which identifies individuals.

If Institute of Education withholds data from you as a result of an exemption under the Data Protection Act, we will explain why the data have been withheld and the relevant exemption, unless doing so would itself disclose information which would be subject to the exemption.

The Data Protection Act allows us to refuse to provide you with a copy of your data if the effort in doing so would be disproportionate, or if the same or similar data have already been provided to you and a reasonable interval has not elapsed since your previous subject access request. In addition, if Institute of Education reasonably requires further information from you in order to locate the data which you have requested, and we inform you of this, we are not required to comply with your request until you supply us with the information.

We have to protect the Data Protection rights and other legal rights of other individuals when we respond to subject access requests. Information which does not relate to you may be 'blacked out' or edited out, particularly if it relates to other individuals. Sometimes we may not be able to release data relating to you because doing so would also reveal information about other persons who have not consented to their data being released, and it would not be reasonable in the circumstances to release the data without their consent. In such cases, you will be informed that data about you have been withheld and the reasons for doing so.

### **3. How has Freedom of Information affected Data Protection?**

The Freedom of Information Act 2000 has amended the Data Protection Act to provide individuals with additional rights in regard to personal data held by public authorities, such as Institute Of Education, to which the Freedom of Information Act applies. In particular, you can now gain access to "manual" (i.e. non-electronic) data about you regardless of how the filing or record keeping system containing the data is organized. However, this right is subject to certain limitations:

- If you require access to "unstructured" manual data (i.e. data held in a system which is not organized in such a way that specific categories of information about you can be easily located), you must describe the information in a way which allows us to find it. A general request such as "please send me all of the data which you hold about me" is not sufficient, in terms of access to unstructured manual data, and will lead us to contact you for further information.
- We are not obliged to provide you with access to unstructured manual data if the cost of locating and extracting the information would exceed the "appropriate limit" set by the Freedom of Information Act for Freedom of Information Act requests. For organizations like Institute Of Education, this is currently £450 or 18 hours of staff time.

#### **4. How do I submit a request?**

Requests for access to personal data must be in writing. We ask that you complete and return Institute of Education's subject access request form, which is designed to gather the information which we need to identify you, communicate with you and locate data about you. Please find a copy of the form attached with this email. Failure to complete the form fully could delay processing of your request, as we may need to contact you for further information or clarification.

You must also send us a fee of £10 (payable to the Institute of Education), and proof of your identity. We will not begin processing your request until the fee and proof of ID are received. We require proof of ID to ensure that we are releasing data to the correct person. Please supply a photocopy (**not** the original) of one of the following:

- The pages which identify you in your passport.
- Your driving licence.

Please send the completed subject access request form, fee and proof of identity by post to the following address:

Matthew Grigson  
Assistant Secretary/ Records Manager  
20 Bedford Way  
London WC1H 0AL

The form, fee and proof of identity must be submitted for each subject access request.

We will be able to process your request more quickly if you provide us with as much information as possible about the data which you are seeking. For example, if you only want data relating to your academic record, you should indicate this to avoid all data relating to you from being searched.

#### **5. What happens next?**

We will send you an acknowledgement of your request as soon as possible. This will indicate the deadline by when we will send you a response. We may also ask you to provide further information or clarification if we require it to process your request, and may contact you again for additional information or clarification if necessary.

After the Institute of Education receives your request, we must consider it and respond to it. We will respond as soon as possible, and in all cases within 40 calendar days of receipt of your request. If we reasonably require further information from you to locate the data which you have requested, we will inform you as soon as possible, and the 40 day deadline will commence from the date when we receive the information from you.

Any copies of data which are provided to you must be in permanent form. We will normally send the data on paper to the postal address specified by you on the subject access request form, unless we agree with you that the data can be supplied in a

different format. The data may take the form of photocopies, printouts, transcripts or extracts, or a combination of these, depending on what is most appropriate in the circumstances. Although you do not have a right to inspect original documents, we may offer this to you where supplying you with copies of the data would involve disproportionate effort.

If Institute of Education holds no data about you, you will be informed of this. You will also be informed of any cases where data about you have been withheld and the reasons for this, including the relevant exemptions (see 2 above.), unless doing so would itself reveal information which would be subject to an exemption.

## **6. Can I appeal?**

You can ask for an internal review of your case if the Institute of Education refuses your subject access request or you are dissatisfied with the handling of your request. Appeals should be sent in writing to the Director of Administration at the following address:

Director of Administration  
20 Bedford Way  
London WC1H 0AL  
Fax: +44 (0)20 7898 6089  
Email: [directoradmin@ioe.ac.uk](mailto:directoradmin@ioe.ac.uk)

The Director of Administration will acknowledge your appeal within seven working days, and will convene a panel to investigate it. A response will be sent to you within 40 working days of receipt of your appeal. If it includes a decision that data should be released to you, the information will be provided to you as soon as possible.

You can also ask the Information Commissioner for an assessment as to whether Institute of Education has processed your data in accordance with the Data Protection Act. The Commissioner can be contacted at the following address:

Information Commissioner  
Wycliffe House  
Water Lane  
Wilmslow  
Cheshire SK9 5AF  
United Kingdom

## Institute of Education, University of London

**Subject Access Request****Request for personal data under the Data Protection Act 1998**

Please complete and return this form together with your fee and proof of identity to the Institute of Education's Records Manager.

<b>Surname:</b>	<b>Forename(s):</b>
<b>Former Surname(s)</b> (if applicable):	
<b>Postal Address:</b>	
<b>Post Code:</b>	<b>Country:</b>
<b>Daytime telephone:</b>	<b>Email:</b>
<b>Date of Birth</b> (for identification purposes only):	
<b>Please indicate your relationship with the Institute of Education:</b>	
Current Student	
Former Student	
Current Staff Member	
Former Staff Member	
Other (Please detail):	
<b>Data requested</b> (Please describe the data which you are seeking as precisely as you can. The more precise you can be the better able we will be able to help you. Continue on a separate sheet if necessary):	

**Statement**

I certify that I am the person named on this form and that I wish to be provided with the date which I have specified relating to myself under the Data Protection Act 1998. I will not publish any data which are supplied to me without prior permission from the Institute of Education or the copyright owner (of copyright is not owned by the Institute of education), except where permitted by law.

**Signature:****Date:**

Please enclose the following with this form:

- a fee of £10 (payable to the Institute of Education),

and proof of your identity. Please supply a photocopy (**not** the original) of one of the following:

- The pages which identify you in your passport.
- Your driving licence.

Please send the completed subject access request form, fee and proof of identity by post to the following address:

Matthew Grigson  
Assistant Secretary/ Records Manager  
20 Bedford Way, London WC1H 0AL

**Data Protection Act Declaration:** The data gathered by this form will be used to process your request under the Data Protection Act. It will be held by the Records Manager, and may be transferred to other parts of the Institute of Education for the purposes of verifying your identity or processing your request for data. The data will be held for six years from the date when we responded to your request, unless your request forms part of an ongoing case, in which case the data will be kept for as long as is necessary.

**SAR information summary sheet**

This sheet is to be completed by data holders in relation to Subject Access Requests and submitted to the Records Managers along with a copy of all records held.

**Name of Subject:**

<b>Ref No.</b>	<b>Description of the data held</b> (e.g. correspondence re: ..., application form, tutors notes)	<b>Purpose of holding the data</b> (Why is it held, how is it processed? N.B. if not clear from the description)	<b>Source of the data</b> (N.B. if not clear from the description)	<b>Disclosure</b> (Who has been given access to the data? N.B. if not clear from the description)	<b>Format (s) of data held</b> (e.g. paper, electronic - word, excel, database file N.B. if not clear from the description)

### Research Data Security

#### Fair and Lawful Processing

1. The fair processing code requires that a research subject is informed of :
  - the identity of the data controller & any nominated representative,
  - the purposes for which the personal data is to be processed,
  - any further information (e.g., intended disclosures or retention times) which is necessary to ensure that processing is fair.
2. This information should be included on any form used to collect personal data. In most cases the data controller will be the Institute of Education. (Individuals in the research team need not be identified.)
3. Research subjects must give informed consent. The amount of detail needed will vary. In some cases, implied consent may be sufficient (for example by return of a questionnaire), in others, clear written consent is required. **Sensitive data** (physical or mental health, race or ethnic origin, religious or political beliefs, trade union membership, criminal convictions) **always require explicit written consent.**
4. If data are obtained from third parties then the third parties must also be properly briefed about the research.
5. Where it is not "necessary" to process personal data (because identifying features can be removed), then they should be anonymised.

#### Security

6. Security must be appropriate to the nature of the data to be protected. In the health and social sciences fields, research data will almost inevitably include "sensitive" information, which requires the highest level of security and confidentiality. The required levels of security must be maintained throughout processing - at University, at the premises of delegated data processors, at home, on laptops, etc.
7. If the project involves a group of personnel, one member should be responsible for overall data security and should control who has data access, for how long and at what level. This could be an administrator who need not necessarily have full access him- or herself.
8. *Delegation of data processing by the data holder to others* (e.g., for scanning, transcription, or statistical analysis): Data holders must ensure that all data processors, including temporary employees, or staff who have been asked to undertake work in their own time, are required to sign a standard form, relating to compliance with confidentiality and security requirements.

9. Recommended security measures:

- There should be a suitable lock on the door to a research unit.
- Manual data should be stored in a locked facility when not under the direct supervision of a data holder or processor, including
  - questionnaires,
  - notes and other paper files,
  - audio- and videotapes,
  - photographs and negatives,
  - removal digital media (e.g. memory sticks, CD/DVD roms, Floppy and zip disks, external hard drives).

10. Access to data stored on a computer should be controlled by passwords and, where appropriate, access to individual files should also be password-protected. Passwords should be known only to authorised people and changed at regular intervals. (Password protection may not be enough to keep data safe from hackers; data encryption should be considered where possible.)

11. Do not leave a PC unattended with an active, password-protected program still running.

12. Back up research data regularly. Back up files should be kept on a secure shared drive, rather than removal digital media (for help in accessing such a drive, consult your IT technician). When working at home or on a laptop, the opposite is true: personal data should be kept on password-protected media and not on the hard drive of a home PC or a laptop.

13. All removal digital media (e.g. memory sticks, CD/DVD roms, Floppy and zip disks, external hard drives) must be password-protected and disposed of securely. Keep in mind the potential damage to individuals which may result if a disk is lost or stolen.

14. When staff work at home, security should be of the same standard as that which is provided in the university. Consider the following:

- access of other individuals (e.g., family members) to the PC, to other automated data (e.g., digital images), or to paper files;
- protection against theft or loss (of the PC, disks, memory sticks, tapes, digital cameras, laptops, mobile telephones);
- back up provisions.

15. Consider the security of data 'on the move', e.g., e-mail, posting work to a co-researcher, using a laptop, etc. If possible, use or initiate 'safe-haven' procedures for such communications, e.g., locate the fax machine or

printer in a lockable room with restricted access. If no 'safe-haven' is available, omit identifying data from the fax, provide numbers instead, and then telephone with the 'missing' data. In the case of e-mail, send personal information in an attachment which has been password-protected and communicate the password by telephone or by separate email.

16. Email should not be used for confidential or "sensitive" data (unless encryption is used).

### **Retention & Disposal**

17. Personal data must be disposed of securely:

- printed material should be shredded and/or burnt,
- tapes and disks must be completely cleaned before re-use,
- computers must be completely cleared of data before disposal or use for other purposes (This procedure also applies when a University laptop is being borrowed.),
- any breaches of security must be investigated and remedied.

**NB:** Simply deleting files from a computer, laptop or removal digital media not sufficient to remove data completely; multiple re-formatting is necessary to ensure that data are irretrievable.

18. Make plans for the storage and disposal of data when the research project is finished.

19. Partial exemption for research data: Information collected for the purpose of one piece of academic research can be used for other research, without breaching the "specified processing" principle, and can be kept indefinitely. For example, staff and students involved in academic research can keep records of questionnaires and contacts, so that the research can be revisited at a later date, or so that, in support of a research project looking at an associated area, they can re-analyse the data.



## Data Protection Register - Entry Details

---

**Registration Number: Z6020689**

**Date Registered:** 11 February 2002      **Registration Expires:** 10 February 2009

**Data Controller:** INSTITUTE OF EDUCATION, UNIVERSITY OF LONDON

**Address:**  
20 BEDFORD WAY  
LONDON  
WC1H 0AL

---

**This register entry describes, in very general terms, the personal data being processed by:**

INSTITUTE OF EDUCATION, UNIVERSITY OF LONDON

**This register entry contains personal data held for 11 purpose(s)**

---

### **Purpose 1**

Staff, Agent and Contractor Administration

### **Data Controllers further description of Purpose:**

THE ADMINISTRATION OF PROSPECTIVE, CURRENT AND PAST EMPLOYEES INCLUDING SELF-EMPLOYED, CONTRACT PERSONNEL, TEMPORARY STAFF OR VOLUNTARY WORKERS;  
ADMINISTRATION OF NON-UNIVERSITY STAFF CONTRACTED TO PROVIDE SERVICES ON BEHALF OF THE UNIVERSITY;  
PLANNING AND MANAGEMENT OF DATA CONTROLLERS WORKLOAD OR BUSINESS ACTIVITY;  
OCCUPATIONAL HEALTH SERVICE;  
ADMINISTRATION OF AGENTS OR OTHER INTERMEDIARIES;  
PENSIONS ADMINISTRATION;  
DISCIPLINARY MATTERS, EMPLOYMENT TRIBUNALS ETC;

STAFF TRAINING;  
VETTING CHECKS.

**Data subjects are:**

Staff including volunteers, agents, temporary and casual workers  
Customers and clients  
Suppliers  
Relatives, guardians and associates of the data subject  
Advisers, consultants and other professional experts  
Previous and prospective employers of the staff and referees  
Agents and contractors

**Data classes are:**

Personal Details  
Family, Lifestyle and Social Circumstances  
Education and Training Details  
Employment Details  
Financial Details  
Goods or Services Provided  
Racial or Ethnic Origin  
Trade Union Membership  
Physical or Mental Health or Condition  
Offences (Including Alleged Offences)  
CUSTOMER, CLIENT DETAILS (INCLUDING GOODS, SERVICES RECEIVED);  
SUPPLIER DETAILS (INCLUDING GOODS, SERVICES PROVIDED).

**Sources (S) and Disclosures (D)(1984 Act). Recipients (1998 Act):**

RECIPIENTS OF UNIVERSITY SERVICES;  
HIGHER EDUCATION STATISTICS AGENCY;  
STUDENT UNION;  
LEGAL REPRESENTATIVES.  
Data subjects themselves  
Relatives, guardians or other persons associated with the data subject  
Current, past or prospective employers of the data subject  
Healthcare, social and welfare advisers or practitioners  
Education, training establishments and examining bodies  
Employees and agents of the data controller  
Suppliers, providers of goods or services  
Financial organisations and advisers  
Survey and research organisations  
Police forces  
Local Government  
Central Government  
Courts / Tribunals  
Careers service  
Trade unions and staff associations

**Transfers:**

None outside the European Economic Area

---

**Purpose 2**

Advertising, Marketing, Public Relations, General Advice Services

**Data Controllers further description of Purpose:**

THE IDENTIFICATION OF RECIPIENTS FOR UNIVERSITY SERVICES AND ADMINISTRATION OF PROMOTIONAL CAMPAIGNS;  
THE ADVERTISING AND PROMOTION OF THE UNIVERSITY AND ITS SERVICES INCLUDING BY DIRECT MARKETING MEANS;  
THE ADVERTISEMENT AND PROVISION OF GENERAL ADVICE TO MEMBERS OF THE PUBLIC ABOUT UNIVERSITY SERVICES;  
THE ADVERTISEMENT AND PROMOTION OF THE UNIVERSITY THROUGH THIRD PARTY PRODUCTS AND SERVICES E.G. FINANCIAL SPONSORSHIP;  
FUNDRAISING FOR THE UNIVERSITY AND OTHER ORGANISATIONS (EXCLUDING FUNDRAISING THROUGH ALUMNI.

**Data subjects are:**

Staff including volunteers, agents, temporary and casual workers  
Customers and clients  
Complainants, correspondents and enquirers  
Relatives, guardians and associates of the data subject  
Advisers, consultants and other professional experts  
Students and pupils  
PERSONS WHO MAY BE SUBJECT OF ENQUIRY, PRESS RELEASE OR OTHER PROMOTIONAL EXERCISE;  
DONORS AND FRIENDS OF THE UNIVERSITY.

**Data classes are:**

Personal Details  
Family, Lifestyle and Social Circumstances  
Education and Training Details  
Employment Details  
Physical or Mental Health or Condition  
CUSTOMER, CLIENT DETAILS (INCLUDING GOODS, SERVICES RECEIVED);  
SUPPLIER DETAILS (INCLUDING GOODS, SERVICES PROVIDED).

**Sources (S) and Disclosures (D)(1984 Act). Recipients (1998 Act):**

RECIPIENTS OF UNIVERSITY SERVICES;  
STUDENT UNION.

Data subjects themselves

Relatives, guardians or other persons associated with the data subject

Current, past or prospective employers of the data subject

Employees and agents of the data controller

Suppliers, providers of goods or services

Persons making an enquiry or complaint

Trade, employer associations and professional bodies

The media

Trade unions and staff associations

**Transfers:**

Worldwide

---

**Purpose 3**

Accounts & Records

**Purpose Description:**

Keeping accounts related to any business or other activity carried on by the data controller, or deciding whether to accept any person as a customer or supplier, or keeping records of purchases, sales or other transactions for the purpose of ensuring that the requisite payments and deliveries are made or services provided by him or to him in respect of those transactions, or for the purpose of making financial or management forecasts to assist him in the conduct of any such business or activity

**Data Controllers further description of Purpose:**

THE ADMINISTRATION OF SUPPLIER RECORDS RELATING TO GOODS,  
ORDERS, SERVICES AND  
ACCOUNTS PROVIDED TO THE UNIVERSITY.

**Data subjects are:**

Staff including volunteers, agents, temporary and casual workers

Suppliers

Advisers, consultants and other professional experts

Students and pupils

**Data classes are:**

Personal Details

Employment Details

Financial Details  
Goods or Services Provided

**Sources (S) and Disclosures (D)(1984 Act). Recipients (1998 Act):**

Data subjects themselves  
Business associates and other professional advisers  
Employees and agents of the data controller  
Suppliers, providers of goods or services  
Persons making an enquiry or complaint  
Financial organisations and advisers  
Central Government  
Auditors  
Courts / Tribunals

**Transfers:**

None outside the European Economic Area

---

**Purpose 4**

Education

**Purpose Description:**

The provision of education or training as a primary function or as a business activity.

**Data Controllers further description of Purpose:**

ADMINISTRATION OF EDUCATION AND TRAINING (E.G. REGISTRATION AND MONITORING, CALCULATION AND PUBLICATION OF EXAM RESULTS, PROVISION OF REFERENCES);  
PROVISION OF EDUCATION AND TRAINING (E.G. PLANNING AND CONTROL OF CURRICULA AND EXAMS, COMMISSIONING, VALIDATING AND PRODUCING EDUCATIONAL MATERIALS, SANDWICH PLACEMENTS);  
ADMINISTRATION OF APPLICATIONS (E.G. RECEIPT AND PROCESSING OF UCAS FORMS, COMPILATION OF STATISTICS, ASSESSMENTS INCLUDING PRELIMINARY AND CONFIRMED OFFERS, LIASON WITH UCAS);  
PREPARATION OF DFEE RETURNS;  
ADMINISTRATION OF STUDENT AWARDS AND FEES.  
GENERAL TEACHING COUNCIL RETURNS  
TTA RETURNS

HESA RETURNS  
HEFCE RETURNS

**Data subjects are:**

Staff including volunteers, agents, temporary and casual workers  
Suppliers  
Complainants, correspondents and enquirers  
Relatives, guardians and associates of the data subject  
Advisers, consultants and other professional experts  
Students and pupils  
AUTHORS, PUBLISHERS, EDITORS, ARTISTS AND OTHER CREATORS;  
THIRD PARTIES PARTICIPATING IN COURSE WORK E.G. VOLUNTEERS,  
PATIENTS,  
SURVEY RESPONDENTS.

**Data classes are:**

Personal Details  
Family, Lifestyle and Social Circumstances  
Education and Training Details  
Employment Details  
Financial Details  
Racial or Ethnic Origin  
Religious or Other Beliefs Of A Similar Nature  
Physical or Mental Health or Condition  
Offences (Including Alleged Offences)  
STUDENT RECORDS;  
SUPPLIER DETAILS (INCLUDING GOODS, SERVICES PROVIDED).

**Sources (S) and Disclosures (D)(1984 Act). Recipients (1998 Act):**

UCAS;  
FUNDING COUNCILS;  
HIGHER EDUCATION STATISTICS AGENCY;  
STUDENT UNION.  
Data subjects themselves  
Relatives, guardians or other persons associated with the data subject  
Current, past or prospective employers of the data subject  
Healthcare, social and welfare advisers or practitioners  
Education, training establishments and examining bodies  
Employees and agents of the data controller  
Suppliers, providers of goods or services  
Financial organisations and advisers  
Survey and research organisations  
Police forces  
Local Government  
Voluntary and charitable organisations  
The media

Courts / Tribunals  
Department for education and employment

**Transfers:**

Worldwide

---

**Purpose 5**

Student and Staff Support Services

**Data Controllers further description of Purpose:**

ADMINISTRATION AND MANAGEMENT OF UNIVERSITY AND PRIVATELY OWNED PROPERTY (INCLUDING ACCOMMODATION SERVICES);  
ADMINISTRATION OF GRANTS AND LOANS (E.G. STUDENT LOANS, LOANS FROM THE STUDENT LOAN COMPANY, ACCESS LOANS);  
ADMINISTRATION AND PROVISION OF HEALTH CARE SERVICES;  
ADMINISTRATION AND PROVISION OF LIBRARY SERVICES (INCLUDING MEMBERSHIP RECORDS, LOAN/HIRE RECORDS, INFORMATION AND DATABANK ADMINISTRATION);  
TICKET ISSUE/RESERVATION SERVICES;  
ADMINISTRATION AND PROVISION OF A STUDENT CARD;  
ADMINISTRATION AND PROVISION OF WELFARE AND PASTORAL SERVICES;  
CAREERS GUIDANCE;  
PROVISION OF CRECHE FACILITIES;  
ADMINISTRATION AND PROVISION OF COMPUTING FACILITIES.

**Data subjects are:**

Staff including volunteers, agents, temporary and casual workers  
Suppliers  
Complainants, correspondents and enquirers  
Relatives, guardians and associates of the data subject  
Advisers, consultants and other professional experts  
Students and pupils  
Business or other contacts  
Landlords  
Tenants  
HEALTH PROFESSIONALS;  
WELFARE AND PASTORAL PROFESSIONALS AND ADVISORS;  
AUTHORS, CONSULTANTS, OTHER PROFESSIONAL EXPERTS;  
SUBJECTS OF RESEARCH;  
FINANCIAL SPONSORS.

**Data classes are:**

Personal Details  
Family, Lifestyle and Social Circumstances  
Education and Training Details  
Employment Details  
Financial Details  
Goods or Services Provided  
Racial or Ethnic Origin  
Religious or Other Beliefs Of A Similar Nature  
Trade Union Membership  
Physical or Mental Health or Condition  
Sexual Life

**Sources (S) and Disclosures (D)(1984 Act). Recipients (1998 Act):**

STUDENT LOANS COMPANY LTD;  
PRISON SERVICE;  
PROBATION SERVICE;  
STUDENT UNION;  
PUBLIC UTILITIES.  
Data subjects themselves  
Current, past or prospective employers of the data subject  
Education, training establishments and examining bodies  
Business associates and other professional advisers  
Employees and agents of the data controller  
Financial organisations and advisers  
Local Government  
The media  
Courts / Tribunals  
Careers service  
Trade unions and staff associations  
Department of social security  
Landlords

**Transfers:**

Worldwide

---

**Purpose 6**

Research

**Purpose Description:**

Research in any field, including market, health, lifestyle, scientific or technical research.

**Data Controllers further description of Purpose:**

ACADEMIC RESEARCH OR STATISTICAL ANALYSIS IN ALL FIELDS,  
INCLUDING SCIENTIFIC,  
TECHNICAL, HEALTH, SOCIAL, ECONOMIC OR MARKET RESEARCH;  
IDENTIFICATION OF SUBJECTS FOR SURVEY OR ANALYSIS;  
COLLECTION OR EXTRACTION OF DATA;  
ANALYSIS, INTERPRETATION AND EVALUATION OF DATA;  
OUTPUT/PRESENTATION OF RESULTS OR FINDINGS;  
ADMINISTRATION OF RESEARCH FUNDING.

**Data subjects are:**

Staff including volunteers, agents, temporary and casual workers  
Customers and clients  
Suppliers  
Complainants, correspondents and enquirers  
Relatives, guardians and associates of the data subject  
Advisers, consultants and other professional experts  
Students and pupils  
SUBJECTS OF RESEARCH;  
FINANCIAL SPONSORS.

**Data classes are:**

Personal Details  
Family, Lifestyle and Social Circumstances  
Education and Training Details  
Employment Details  
Financial Details  
Goods or Services Provided  
Racial or Ethnic Origin  
Religious or Other Beliefs Of A Similar Nature  
Trade Union Membership  
Physical or Mental Health or Condition  
Offences (Including Alleged Offences)

**Sources (S) and Disclosures (D)(1984 Act). Recipients (1998 Act):**

PROVIDERS OF PUBLICLY AVAILABLE INFORMATION;  
FINANCIAL SPONSORS.  
Data subjects themselves  
Education, training establishments and examining bodies  
Employees and agents of the data controller  
Suppliers, providers of goods or services  
Persons making an enquiry or complaint  
Financial organisations and advisers  
Survey and research organisations  
Customers and clients of the data controller for goods and services

**Transfers:**

Worldwide

---

## **Purpose 7**

Other Commercial Services

### **Data Controllers further description of Purpose:**

THE PROVISION OF CONSULTANCY AND ADVISORY SERVICES;  
PROVISION OF CONFERENCE FACILITIES (E.G. LECTURE HALLS,  
ACCOMMODATION,  
CATERING ETC.);  
OTHER CHARGEABLE SERVICES (EXCLUDING TUITION FEES).

### **Data subjects are:**

Staff including volunteers, agents, temporary and casual workers  
Customers and clients  
Suppliers  
Complainants, correspondents and enquirers  
Relatives, guardians and associates of the data subject  
Advisers, consultants and other professional experts  
Students and pupils

### **Data classes are:**

Personal Details  
Employment Details  
Financial Details  
Goods or Services Provided

### **Sources (S) and Disclosures (D)(1984 Act). Recipients (1998 Act):**

Data subjects themselves  
Suppliers, providers of goods or services  
Persons making an enquiry or complaint  
Financial organisations and advisers  
Debt collection and tracing agencies  
The media  
Courts / Tribunals  
Customers and clients of the data controller for goods and services

### **Transfers:**

Worldwide

---

## **Purpose 8**

Method 2

**Data Controllers further description of Purpose:**

PUBLICATION OF THE UNIVERSITY MAGAZINE

**Data subjects are:**

Staff including volunteers, agents, temporary and casual workers  
Students and pupils

**Data classes are:**

Personal Details  
PHOTOGRAPHIC IMAGES;  
TEXT OF MAGAZINE ARTICLES.

**Sources (S) and Disclosures (D)(1984 Act). Recipients (1998 Act):**

STUDENTS AND PUPILS  
Data subjects themselves  
The media

**Transfers:**

None outside the European Economic Area

---

**Purpose 9**

Crime Prevention and Prosecution of Offenders

**Purpose Description:**

Crime prevention and detection and the apprehension and prosecution of offenders.

**Data Controllers further description of Purpose:**

INCLUDES USE OF CCTV (THE USE OF CLOSED-CIRCUIT TELEVISION FOR THE MONITORING AND COLLECTION OF SOUND AND/OR VISUAL IMAGES FOR THE PURPOSE OF MAINTAINING THE SECURITY OF PREMISES, FOR PREVENTING CRIME AND FOR INVESTIGATING CRIME)

**Data subjects are:**

Customers and clients  
Offenders and suspected offenders  
MEMBERS OF THE PUBLIC.

**Data classes are:**

Personal Details  
Goods or Services Provided  
Offences (Including Alleged Offences)  
Criminal Proceedings, Outcomes And Sentences.

**Sources (S) and Disclosures (D)(1984 Act). Recipients (1998 Act):**

SECURITY ORGANISATIONS  
Data subjects themselves  
Business associates and other professional advisers  
Employees and agents of the data controller  
Suppliers, providers of goods or services  
Persons making an enquiry or complaint  
Police forces

**Transfers:**

None outside the European Economic Area

---

**Purpose 10**

Method 2

**Data Controllers further description of Purpose:**

ALUMNI RELATIONS:  
THE PROMOTION OF THE RELATIONSHIP BETWEEN THE UNIVERSITY  
AND IT'S ALUMNI;  
UNIVERSITY-RELATED FUNDRAISING INITIATIVES INVOLVING ALUMNI;  
ADVERTISING AND PROMOTION OF ALUMNI EVENTS AND REUNIONS;  
DISTRIBUTION OF UNIVERSITY MAILINGS (E.G. ALUMNI MAGAZINES,  
NEWSLETTERS,  
ANNUAL REPORTS) AND MESSAGE FORWARDING (WITHOUT  
DISCLOSURE OF DATA);  
THE PROMOTION OF BENEFITS AND SERVICES AVAILABLE TO ALUMNI  
FROM THIRD PARTIES;  
ELICITING NON-FINANCIAL SUPPORT (E.G. CAREERS ADVICE TO  
STUDENTS, HELP WITH  
STUDENT RECRUITMENT).

**Data subjects are:**

Staff including volunteers, agents, temporary and casual workers  
Suppliers  
Relatives, guardians and associates of the data subject  
Students and pupils  
Donors and lenders  
ASSOCIATES, FRIENDS OF THE UNIVERSITY;  
CUSTOMERS, CLIENTS OF THE UNIVERSITY.

**Data classes are:**

Personal Details  
Family, Lifestyle and Social Circumstances  
Education and Training Details  
Employment Details  
Financial Details  
Goods or Services Provided  
Racial or Ethnic Origin  
STUDENT RECORD.

**Sources (S) and Disclosures (D)(1984 Act). Recipients (1998 Act):**

UNIVERSITY AFFILIATED/ASSOCIATED GROUPS;  
RECIPIENTS OF UNIVERSITY SERVICES;  
STUDENT UNION.  
Data subjects themselves  
Relatives, guardians or other persons associated with the data subject  
Employees and agents of the data controller  
Suppliers, providers of goods or services  
Financial organisations and advisers

**Transfers:**

Worldwide

---

**Purpose 11**

Crime Prevention and Prosecution of Offenders

**Purpose Description:**

Crime prevention and detection and the apprehension and prosecution of offenders.

**Data subjects are:**

Staff including volunteers, agents, temporary and casual workers  
Customers and clients  
Suppliers  
Members or supporters

Complainants, correspondents and enquirers  
Relatives, guardians and associates of the data subject  
Advisers, consultants and other professional experts  
Students and pupils  
Offenders and suspected offenders

**Data classes are:**

CCTV IMAGES

**Sources (S) and Disclosures (D)(1984 Act). Recipients (1998 Act):**

Data subjects themselves  
Employees and agents of the data controller  
Other companies in the same group as the data controller  
Police forces

**Transfers:**

None outside the European Economic Area

---

**Statement of exempt processing:**

This data controller also processes personal data which is exempt from notification

---

---

Copyright in this copy is owned by the Information Commissioner. Data Controllers may take copies of their own register entries. Apart from that no part of it may be copied unless allowed under the Copyright Designs and Patent Act 1988.

---

[© Copyright](#)