Roehampton University London

ROEHAMPTON UNIVERSITY

DATA PROTECTION POLICY

Originated by: Data Protection Working Group:	*November 2008*
Impact Assessment:	(*to be confirmed)*
Recommended by Senate:	*28 January 2009*
Approved by Council:	*9 March 2009*
Revised:	*28 June 2010*
Review Date:	*March 2012*

ROEHAMPTON UNIVERSITY

DATA PROTECTION POLICY

Background

Roehampton University processes information about its staff, students and other individuals for a variety of purposes. When processing information, the University is committed to protecting the rights and privacy of students, staff and others in compliance with the Data Protection Act 1998 [the 'Act'] and related legislation. This Policy sets out the principles that will apply in meeting this commitment. The accompanying Guidelines on Personal Data provide detail on the application and implementation of the Policy.

Data Controller

The University as a body corporate is the data controller under the Act.

Application of Policy

The Policy and the Data Protection Principles apply to all staff, students and agents of the University, including those who process personal data off-site.

All personal data collected, held and processed on computer, on-line as well as in structured manual files is subject to this Policy and to the Data Protection Principles. Examples of the purposes for which data is processed by the University include but are not limited to: recruiting and paying staff, administering programmes of study, recording progress, calculating and approving awards, collecting fees, and complying with legal obligations to funding bodies and government

Notification[1]

Notification is the responsibility of the University Secretary and Registrar and the Data Protection Officer. Details of the University's notification are published on the Information Commissioner's website. Anyone who is, or intends, processing data for purposes not included in the University's Notification must seek advice from the Data Protection Officer.

Compliance with Policy

The Vice-Chancellor's senior management group, Heads of Departments, Directors and others in managerial or supervisory roles, are responsible for ensuring adherence to this Policy.

A breach of the Act or of this Policy may constitute a disciplinary offence for either staff or students and trigger the application of the relevant disciplinary procedures. A breach of the Act may also constitute a criminal offence. Other agencies and individuals working with the University, and who have access to personal information processed by the University, must also comply with this Policy. Departments and academic units that interact with external agencies are responsible for ensuring that such agencies agree to abide by this policy.

---

[1] Notification is the process by which a data controller informs the Information Commissioner of certain details about their processing of personal information. These details are used by the Information Commissioner to make an entry describing the processing in the register of data controllers that is available to the public for inspection. Notification is a statutory requirement and every organisation that processes personal information must notify the Information Commissioner's Office (ICO), unless they are exempt. Failure to notify is a criminal offence.

DATA PROTECTION PRINCIPLES

The University is committed to complying with the eight Data Protection Principles ("the Principles") in the Act. To that end:

1. **Personal data shall be processed fairly and lawfully.**

2. **Personal data shall be obtained for specific and lawful purposes and not processed in a manner incompatible with those purposes.**
   Personal data should only be obtained if there is a clear purpose or purposes for which it will be used, and must not then be used for a different purpose. Further, personal data may only be processed for purposes identified in the University's notification with the Information Commissioner's Office.

3. **Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is held.**
   Only the information needed for a specific purpose should be collected. If data are given or obtained which are excessive for the purpose, they should be immediately deleted or destroyed.

4. **Personal data shall be accurate and, where necessary, kept up to date.**
   Data that are kept for a long time must be periodically reviewed and updated as necessary. Data should not be kept unless it is reasonable to assume that they are accurate.

   Members of the University are responsible for ensuring that any personal data they supply to the University are accurate and up-to-date.

5. **Personal data shall be kept only for as long as necessary.**
   Personal data should not be kept for longer than the data are required for the purpose for which the data was originally obtained. Personal data must, however, be disposed of in a way that protects the rights and privacy of data subjects (e.g.. shredding, disposal as confidential waste, secure electronic deletion).

6 **Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act.**
   Personal data should not be disclosed to third parties except in circumstances permitted or required by the Act or with the consent of the individual concerned. In most cases, this consent should be provided in writing. Further guidance on how to respond to requests from third parties for the disclosure of personal data is set out below as well as in the Guidelines and FAQs accompanying this Policy.

7. **Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of data.**
   All staff are responsible for ensuring that any personal data that they hold are kept securely.

8. **Personal data shall not be transferred to a country or a territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.**
   Data must not be transferred outside of the European Economic Area (EEA) - the EU Member States together with Iceland, Liechtenstein and Norway - without the explicit consent of the individual.

Disclosure of Data

The University will ensure that personal data are not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the police. The University's Data Protection Officer must be advised of any request for personal data relating to a student or member of staff and information should not be provided. When asked by the Data Protection Officer to provide data, particularly data related to a police enquiry or other authority, members of staff shall do so within the time frame specified.

Personal data may be disclosed only where at least one of the following conditions apply:

- the individual has given their written consent;
- where the disclosure is in the legitimate interests of the institution (e.g. disclosure to staff - personal information can be disclosed to other University employees if it is clear that those members of staff require the information to enable them to perform their jobs);
- where the institution is legally obliged to disclose the data (e.g. HESA and HESES returns, ethnic minority and disability monitoring);
- where disclosure of data is required for the performance of a contract (e.g. informing a student's LA or sponsor of course changes/withdrawal etc).

Explicit consent must be obtained when processing sensitive personal data.

Disclosure is permitted without consent if the information is requested for one or more of the following purposes and the purpose is supported by clear evidence:

- to safeguard national security;
- to prevent or detect crime including the apprehension or prosecution of offenders;
- to assess or collect tax duty;
- to discharge regulatory functions (includes health, safety and welfare of persons at work);
- to prevent serious harm to a third party;
- to protect the vital interests of the individual, this refers to life and death situations.

DEFINITIONS (adapted from Data Protection Act 1998)

Data Subject	Any living individual who is the subject of personal data held by an organisation.
Personal Data	Data relating to a living individual who can be identified from that information or from that data and other information in possession of the data controller. Includes name, address, telephone number, id number. Also includes expression of opinion about the individual, and of the intentions of the data controller in respect of that individual.
Processing	Any operation related to the organisation, retrieval, disclosure and deletion of data and includes: Obtaining and recording data Accessing, altering, adding to, merging, deleting data Retrieval, consultation or use of data Disclosure or otherwise making available of data.
Relevant Filing System	Any paper filing system or other manual filing system which is structured so that information about an individual is readily accessible. Please note that this is the definition of "Relevant Filing System" in the Act. Personal data as defined, and covered, by the Act can be held in any format, electronic (including websites and emails), paper-based, photographic etc. from which the individual's information can be readily extracted.
Sensitive Data	Different from ordinary personal data (such as name, address, telephone) and relates to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, criminal convictions. Sensitive data are subject to much stricter conditions of processing.
Third Party	Any individual/organisation other than the data subject, the data controller (University) or its agents.

Robin Geller
University Secretary and Registrar
Approved: January 2009
Revised: May 2010