UNIVERSITY OF Southampton

Data Protection Policy

Approved by the Council 10 July 2008

UNIVERSITY OF SOUTHAMPTON
DATA PROTECTION POLICY

1. Purpose

1.1 The Data Protection Act 1998 ('the Act') has two principal purposes:

i) to regulate the use by those (known as data controllers) who obtain, hold and process personal data on living individuals, of those personal data; and

ii) to provide certain rights (for example, of accessing personal information) to those living individuals (known as data subjects) whose data is held.

1.2 The cornerstones of the Act are the eight data protection principles, which prescribe:

i) guidelines on the information life-cycle (creation/acquisition; holding; processing; querying, amending, editing; disclosure or transfer to third parties; and destruction ('the life-cycle');

ii) the purpose for which data are gathered and held; and

iii) enshrine rights for data subjects.

The Act applies to the University, the Data Controller for the purposes of the Act, and to anyone who holds personal information in a structured way so that retrieval is easy. The University is fully committed to abiding, not only by the letter, but also by the spirit of the Act, and, in particular, is committed to the observation, wherever possible, of the highest standard of conduct mandated by the Act. This policy has been written to acquaint staff with their duties under the Act and to set out the standards expected by the University in relation to processing of personal data and safeguarding individuals' rights and freedoms.

2. Staff duties

Employees of the University are expected to:

i) acquaint themselves with, and abide by, the Data Protection Principles;

ii) read and understand this policy document;

iii) understand how to conform to the standard expected at any stage in the life-cycle;

iv) understand how to conform to the standard expected in relation to safeguarding data subjects' rights (e.g. the right to inspect personal data) under the Act;

v) understand what is meant by 'sensitive personal data', and know how to handle such data; and

vi) contact the Data Protection Officer if in any doubt, and not to jeopardise individuals' rights or risk a contravention of the Act.

3. The Data Protection Principles

The Data Protection Principles, in summary, are:

I Personal data shall be processed fairly and lawfully.

II 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.

III Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

IV Personal data shall be accurate and, where necessary, kept up to date.

V Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

VI Personal data shall be processed in accordance with the rights of data subjects under this Act.

VII 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.

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

4. Best-practice guidelines for the life-cycle process

4.1 Acquisition of personal data (see Principles 1, 2, 3)

Those wishing to obtain personal data must comply with guidelines issued from time to time by the Data Protection Officer and, in particular, should tell data subjects the purpose(s) for which they are gathering the data, obtain their explicit consent, and inform them that the University will be the data controller for the purposes of the Act and the identities of any other persons to whom the data may be disclosed. If sensitive personal data are being collected, explicit consent is not only best practice, it is mandatory. No more data should be collected than is necessary for the purpose(s) declared.

4.2 Holding/safeguarding/disposal of personal data (see Principles 4, 5 and 7)

Data should not be held for longer than is necessary. The University's and/or Schools'/Professional Services' records management policies should be consulted for guidance on what is necessary for each kind of data. Personal data should be reviewed periodically to check that they are accurate and up to date and to determine whether retention is still necessary.

Adequate measures should be taken to safeguard data so as to prevent loss, destruction or unauthorised disclosure. The more sensitive the data, the greater the measures that need to be taken.

4.3 Processing of personal data (see Principles 1, 2)

In this particular context, 'processing' is used in the narrow sense of editing, amending or querying data. In the context of the Act as a whole, 'processing' is very widely defined to include acquisition, passive holding, disclosure and deletion.

Personal data must not be processed except for the purpose(s) for which they were obtained or for a similar, analogous purpose. If the new purpose is very different, the data subject's consent must be obtained.

4.4 Disclosures and transfers of personal data (see Principles 1, 2, 7, 8)

4.4.1 Disclosures

The University's policy is to exercise its discretion under the Act to protect the confidentiality of those whose personal data it holds.

i) Employees of the University may not disclose any information about applicants, students or other employees, including information as to whether or not any person is or has been an applicant, student or employee of the University unless they are clear that they have been given authority by the University to do so. Particular care should be taken in relation to any posting of personal information on the internet.

ii) No employee of the University may provide references to prospective employers or landlords or others without the consent of the individual concerned. It is therefore essential that where the University is given as a referee, the subject of the reference should provide the University with the necessary notification and consent.

iii) No employee may disclose personal data to the police or any other public authority unless that disclosure has been authorised by the University's Data Protection Officer.

4.4.2 Transfers

Personal data should not be transferred outside the University, and in particular not to a country outside the EEA

i) except with the data subject's consent; or
ii) unless that country's data protection laws provide an adequate level of protection; or
iii) adequate safeguards have been put in place in consultation with the Data Protection officer; or
iv) in consultation with the Data Protection Officer, it is established that other derogations apply.

4.5 Destruction of personal data (see Principles 5 and 7)

Personal data must not be held for longer than necessary; and when such data have been earmarked for destruction, appropriate measures must be taken to ensure that the data cannot be reconstructed and processed by third parties.

5. Data subjects' rights of access

The University is fully committed to facilitating access by data subjects ('applicants') to their personal data, while bearing in mind the need to protect other individuals' rights of privacy.

All applicants will be expected to fill in a Subject Access request form, downloadable from the University's web site. Applicants who are members of the University and have a University login and email account may submit this form via their University email account. In such cases, no further proof of ID will be required. Applicants who are not members of the University, and members of the University who do not submit the form via their University email account, must submit supporting documentation which establishes that they are the data

subject (or where the application is made by a third party on behalf of the data subject, which establishes the third party's identity, that of the data subject and a form of authority signed by the data subject is produced).

The fee for a subject access request is £10. All subject access requests are to be forwarded to the Data Protection Officer, if they have not already been addressed to him or her.

6. Review

This policy will be reviewed periodically to take account of changes in the law and guidance issued by the Information Commissioner.

7. Data protection contacts

For general enquiries about the University's Data Protection Policy and for formal subject access requests under the Act:
Data Protection Officer
Legal Services
Corporate Services
University of Southampton
Highfield
Southampton
S017 1BJ
Telephone: (023) 8059 2400
E-mail: legalservices@soton.ac.uk

8. Disciplinary consequences of this policy

Unlawful obtaining or disclosure of personal data (including the transfer of personal data outside the EEA in contravention of paragraph 4.4.2 above) or any other breach of section 55 of the Data Protection Act 1998 by staff or students will be treated seriously by the University and may lead to disciplinary action up to and including dismissal or expulsion.

Dated 7 May 2008

www.southampton.ac.uk
legalservices@soton.ac.uk
+44(0)23 8059 4684