University of Sunderland

Data Protection Policy

Document Control:

Issued By:	*Freedom of Information and Records Management Group (FIRM)*		
Version	Reason for Change	Author	Date
1.0	*Initial Issue*	*B Dale*	*06/08/10*
1.1	*Amendments from S Kerridge*	*B Dale*	*01/10/10*
1.2	*Amendments from FIRM Group meeting 11.10.10*	*B Dale*	*30/11/10*
1.3	*Amendments from C Gales*	*C Gales*	*13/01/11*
1.4	*Amendments from FIRM Group (13/1/11) and C Gales (8/2/11)*	*FIRM and C Gales*	*08/02/11*
1.5	*Final check*	*B Dale*	*10/03/11*
1.6	*Update to contact details of Data Protection Officer*	*S Flanagan*	*27/03/13*

Version control of a document is vital for good records management and consistency across the whole organisation. The latest version of this document will be made available on the University website, please ensure that you use the most up-to-date version.

University of Sunderland
5. Data Protection Policy

1. Introduction

1.1 In order to comply with its obligations under the EU Data Protection Directive (EC No. 95/46) the Government passed a second Data Protection Act in 1998 ("the Act") bringing it into effect on 24 October 1998:-

"An Act to make new provisions for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information".

2. Aims of the Data Protection Policy

Essentially the Act is designed to protect individuals from any disadvantage that might result from the processing of their personal details. It requires the University to focus on the provisions of the Act relating to personal data processed by the University relating to staff, students and others. The aim of this policy is to explain in summary the University's obligations and how the University will meet those obligations.

3. Compliance.

3.1. The University, its staff and students are required to comply with the provisions of the Act.

3.2 The Act includes a more stringent regime of enforcement and corrective provisions compared to earlier legislation, including provision for compensation to those suffering detriment. The Information Commissioner's Office is the UK's independent authority set up to uphold information rights in the public interest including data privacy for individuals

3.3 The Data Protection Act makes the Information Commissioner responsible for:

- promoting good practice in handling personal data, and giving advice and guidance on data protection;
- keeping a register of organisations that are required to notify him about their information-processing activities;
- helping to resolve disputes by deciding whether it is likely or unlikely that an organisation has complied with the Act when processing personal data;
- taking action to enforce compliance with the Act where appropriate; and
- bringing prosecutions for offences committed under the Act.

4. Data Protection Policy

4.1 As and when they apply to the processing of any personal data, the University will comply with the eight Data Protection Principles (see section 7 of this document).

4.2 The University will ensure that all requests made by a data subject in accordance with the Act, and on payment of the appropriate fee for access to data held about him or her shall be processed fully and expeditiously within the time period prescribed by the Act (normally 40 days from the date of payment of the fee).

4.3 When requested to do so by the data subject, the University will ensure that it complies with the requirement to give a description of:

4.3.1 the personal data of which an individual is the data subject;
4.3.2 the purposes for which the data are to be processed;
4.3.3 the recipients or classes of recipients to which the data are or may be disclosed.

4.4 If the University received a data subject access request it will communicate to the data subject in an intelligible form:

4.4.1 the information consisting of any personal data of which that individual is the data subject, and, if requested
4.4.2 any information available to the University as a source of those data.

4.5 The University will use all reasonable endeavours to ensure that the requirements of the Act are observed.

4.6 The University will give appropriate publicity within the institution to the Act and its requirements.

4.7 The University will provide appropriate training materials to all relevant staff, and ensure that reasonable resources are available for the production and dissemination of such materials.

4.8 The University will ensure that any external bodies which process personal data on its behalf give confirmation, in writing, that they will comply with the requirements of the Act, and that they satisfy the minimum requirements concerning the security of data laid down by the Act and the Information Commissioner.

5. Role and Responsibilities of Staff

5.1 In connection with their duties at or relating to the University:

5.1.1 All staff have responsibility to ensure that they comply with the Data Protection Principles and requirements of the Act;

5.1.2 All Staff will only process personal data to the extent to which they have been expressly authorised by the University;

5.1.3 Staff responsible for the processing of personal data are also responsible for informing the University's Data Protection Officer of any new processing of personal data or any change in the processing of existing personal data;

5.1.4 All staff are responsible for complying with any security procedures implemented by the University;

5.1.5 Academic staff and relevant support staff are responsible for ensuring that students are fully informed about their responsibilities under the Act with regard to coursework and research;

5.1.6 Academic staff and relevant support staff authorising, for the purpose of coursework or research, the processing of personal information by students are responsible for the monitoring of that processing.

6. Role and Responsibilities of Students

6.1 In connection with their academic studies/research:

6.1.1 All students have the responsibility to ensure that they comply with the Data Protection Principles and requirements of the Act;

6.1.2 All students will only construct or maintain files of personal data for use in their academic studies/research with the prior express consent of the appropriate member of staff, such data should only be stored on designated secure storage areas;

6.1.3 All students will only process personal data falling within the scope of approved programmes of studies to the extent to which they have been expressly authorised by the University;

6.1.4 All students are responsible for complying with any security procedures implemented by the University;

6.1.5 All students processing personal data for research purposes must ensure that the processing does not cause, or be likely to cause, substantial damage or distress to data subjects.

7. The Data Protection Principles

7.1 The eight Data Protection Principles are found in Schedule 1 to the Act: The language of the Act is complex; the following list is a simplified summary.

The Principles require that personal data shall be:

1 - processed fairly and lawfully and, in particular, shall not be processed unless the specific conditions referred to in Appendix 1 are met;
2 - obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that or those purposes;

3 - adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
4 - accurate and, where necessary, kept up to date;
5 - not kept for any longer than is necessary for that purpose or those purposes;
6 - processed in accordance with the rights of data subjects under the Act;
7 - and that appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss of, destruction of or damage to, personal data; and
8 - 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.

8. Notification

Notification is a statutory requirement and every organisation that processes personal information must notify the Information Commissioner's Office (ICO), unless they are exempt.

Notification is the process by which a data controller gives the ICO details about their processing of personal information. The ICO publishes certain details in the register of data controllers, which is available to the public for inspection. The University will comply with requirements for notification

9. Relationship with existing policies

This policy has been formulated within the context of the following University policies:

- Records Management Policy
- Freedom of Information and Environmental Information Regulations Policy
- Archive and Retention Policy

10. Responsibilities

The Executive member with overall responsibility for this policy is the Deputy Vice Chancellor (Resources and Corporate Services) and Clerk to the Board of Governors.

The Governance and Records Management Officer is the University's nominated Data Protection Officer (DP Officer) and coordinates subject access requests and provides advice on data protection to the University.

The University Deans of Faculty and Directors of Services have overall responsibility for ensuring that their Service or Faculty comply with the Data Protection Act.

Information Champions have direct responsibility for coordinating compliance with the University's Data Protection Policy and the associated guidance, and coordination of replies to data subject access requests.

All Staff need to have an awareness of this policy and its contents. It will be the responsibility of the University's Faculties and Services to ensure that all staff are aware of their responsibilities and how to seek further guidance when needed. The University will provide appropriate training materials.

9. Policy Review

This policy will be reviewed at 5 year intervals, or after major legislative or organisational change, whichever is the sooner.

This Policy was approved by Executive on 12 April 2011.

10. Further Information

10.1 Data Protection Officer

The Act requires the University to nominate one or more 'data protection supervisor(s)' to oversee the University's compliance with the Act.

The Data Protection Officer at the University is

Steven Flanagan,
Legal, Governance and Business Assurance,
4th Floor Edinburgh Building,
Chester Road,
Sunderland,
SR1 3SD
Tel: 0191 5151 2508
e-mail: Dataprotection@sunderland.ac.uk

10.2 Information Champions

Each Faculty/Service within the University shall nominate an Information Champion to liaise with the Data Protection Officer.

APPENDIX

1 The Conditions for processing personal data

Processing of personal data may only be carried out where at least **one** of the following conditions have been satisfied:

1. the individual had given his or her consent to the processing;
2. the processing is necessary for the performance of a contract with the individual;
3. the processing is required under a legal obligation (except an obligation imposed by a contract);
4. the processing is necessary to protect the vital interests of the individual (matters of life and death);
5. the processing is necessary to carry out public functions;
6. the processing is necessary in order to pursue the legitimate interests of the business (unless prejudicial to the interests of the individual) and is fair and lawful.

2 'Sensitive' Personal Data

Stricter conditions apply to the processing of sensitive personal data. Where such data is being processed not only must the Controller meet the requirements of the data protection principles and the conditions in **1** above, but processing is prohibited unless at least **one** of the following conditions has been satisfied:

Nb – The summary below is taken from the ICO Data Protection Guide issued in Dec 2009.

1. The data subject has given his/her explicit consent to the processing of the personal data;
2. The processing is necessary for compliance with employment law;
3. The processing is necessary in order to protect the vital interests of the data subject or other person;
4. The processing is carried out by a not for profit organisation and does not involve disclosing personal data to a third party unless the individual consents in the course of its legitimate activities (Also extra limitations apply in these cases;
5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject;
6. The processing is necessary for the purpose of, or in connection with any legal proceedings, for the purpose of obtaining legal advice or for establishing, exercising or defending legal rights;
7. The processing is necessary for the administration of justice; or
8. The processing is necessary for medical purposes and is undertaken by a health professional.
9. The processing is necessary for monitoring equality of opportunity is carried out with the appropriate safeguards for the rights of individuals.