Data Protection Policy

1. Introduction

We are committed to protecting the rights and privacy of individuals in accordance with the Data Protection Act 1998 ("the Act").

We have to process certain information about all individuals with whom we have dealings, for our own administrative purposes and to comply with our legal obligations. For example, we need to keep personal data about our employees and students in order to carry out our function as a university.

2. Some Key Definitions

Personal Data
This is information that can identify a living person that is held either electronically or in paper form. This can include student records, staff employment details, audio recordings of lectures and images such as those recorded on CCTV.

Data Controller
The data controller decides how and why personal data is to be used, and is legally required to comply with the Act. The University is the data controller for the personal data it uses.

Data Subject
This is a living individual who is the subject of personal data.

Processing
In relation to personal data, this means obtaining, recording or holding the data or carrying out any operation or set of operations on the data.

3. Data Protection Principles

To comply with the Act, we must follow the eight data protection principles of good information handling. The principles are listed in the annex to this policy.

Compliance with the principles is a legal requirement and applies to all personal data for which we are the data controller. All staff, or any other person we appoint to process personal data on our behalf, must ensure that they follow the data protection principles at all times. This section of the policy contains the key ways in which we will work to ensure we follow these principles:

- Whenever we collect personal data, if it is not already clear, we will explain why we are collecting it and what we are going to use it for. We will also let people know if we are going to pass their data onto other organisations, along with any other details that could help them to understand what we are going to do with their personal data.
• We will only collect and use personal data for specific legitimate purposes, and it will be kept only for as long as we need it for those purposes. We will not collect excessive or irrelevant information.

• We will only use personal data for the direct promotion or marketing of goods and services with the consent of the data subjects.

• Personal data will be accessible only to those people who need to use it as part of their work. We will not ordinarily pass personal information to other organisations, unless we have consent or we are legally required to do so.

• We will have appropriate security measures in place to protect personal data, taking account of the nature of the data and the harm that might be caused if it was lost.

• Unauthorised or unlawful accessing, use or disclosure of personal data could lead to disciplinary action, and in some cases may be considered as gross misconduct. In serious cases, it could even be a criminal offence.

• We will provide appropriate training for all relevant staff and will include awareness training at induction.

• Data subjects have the right to ask for access to the personal data we hold about them, and are entitled to be given copies of that data. We have procedures in place to allow for this right of access.

• Whenever we propose to transfer personal data outside of the European Economic Area, we will assess the safeguards that are in place to satisfy the eighth data protection principle.

4. Notification
We have a current and up-to-date entry on the Information Commissioner’s Register of Data Controllers, which notifies the purposes for which we process personal data. This will be reviewed and renewed on an annual basis.

5. Roles and Responsibilities

University Registrar
The University Registrar has overall responsibility for ensuring that the University’s legal obligations are met and has responsibility for internal and external governance and corporate accountability. The University Registrar has been designated as the officer with overall responsibility for policy compliance.

Information Security Officer (Compliance)
• Advise on policy and best practice
• Draw up guidance material in line with best practice
Promote policy compliance
Coordinate and respond to data protection access requests received by the University
Ensure the data protection notification is renewed annually

Senior Managers
Senior managers all have a responsibility for ensuring that data protection issues within their areas are managed in a way that meets the provisions of this policy.

All staff
- Be aware of the Data Protection Act and what it means to the University
- Follow the policy and procedures for handling personal data
- Consult with the Information Security Officer (Compliance) for advice and guidance when necessary

All students
- Check that any personal data provided to the University is accurate and up to date
- Inform us of any changes to their personal data, such as change of address
- Inform us of any errors in their personal data
- Students who intend to use University computer facilities to process personal data must notify, as appropriate, their course tutor, project supervisor or individual supervisor to make sure (before any processing takes place) that any proposed data collection or processing meets the requirements of the Data Protection Act.

6. Relationship with Existing Policies

Related policies and guidance documents are as follows:
- Records Management Policy
- University Records Retention Schedule
- Email Retention and Usage Policy
- Email Etiquette Guidance
- Managing Emails as Records Guidance
- Freedom of Information Policy

7. Authority and Review

This policy was approved at a meeting of Council held on 12 December 2011 and is effective as of that date. The policy will be reviewed periodically.

A breach of this policy could result in disciplinary proceedings.

Steve Williams, Director of University IT
22 November 2011
Annex

Note: that details of the Data Protection Act and the Schedules referred to below can be found at:

The Data Protection Principles

First Principle: Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-
   a) at least one of the conditions in Schedule 2 is met, and
   b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is met.

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 purposes.

Third Principle: Personal data shall be adequate, relevant and not excessive in relation to the purpose or 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 protection for the rights and freedoms of data subjects in relation to the processing of personal data.