

Data Protection Policy

Introduction

The University needs to keep a certain information about its employees, students and other users to allow it to monitor performance, achievements, and health and safety, for example. It is also necessary to process information service staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with.

To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the University must comply with the data protection principles which are set out in the Data Protection Act 1998. In summary, these state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with the purpose.
- Be adequate, relevant and not excessive for those purposes.
- Be accurate and kept up-to-date.
- Not be kept for longer than is necessary for the purpose.
- Be processed in accordance with the data subjects writes.
- Be kept safe from unauthorised access, accidental loss or destruction.
- Not be transferred to a country outside the European economic area, unless the country has equivalent levels of protection for personal data.

The University and all staff or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure this happens, the University has developed the data protection policy.

Status of policy

This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the policies made by the University from time to time. Any failure to follow the policy may therefore result in disciplinary proceedings.

Any member of staff, who considers that the policy has not been followed in respect of personal data about himself, should raise the matter with the designated data controller initially. If the matter is not resolved it should be raised as a formal grievance.

Notification of data held and processed.

All staff, students and other users are entitled to:

- Know what information the University holds and processes about the and why.
- Know how to gain access to it.
- Know how to keep it up-to-date.
- Know what the University is doing to comply with its obligations under the 1998 Act.

The University of therefore provide all staff and students and other relevant users with a standard form of notification. This will state at all the types of data the University holds and processes about them, and the reasons for which it is processed. The University will try to do this at least once every year for staff or on request, and on request for other users.

Responsibilities of staff

All staff are responsible for

- Checking that any information they provide to the University in connection with their employment is accurate and up-to-date.
- Informing the University of any changes to information which they have provided e.g. changes of address
- Checking the information that the University will send out from time to time, giving details of information kept and processed about staff.
- Informing the University of any errors or changes. The University cannot be held responsible for any errors unless the staff member has informed the University.

If and when, as part of their responsibilities, staff collect information about other people, (i.e. about students course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff, which are in the document "Guidelines for Staff on the Data Protection Act 1998".

Data security

All staff are responsible for ensuring that:

- Personal data which they hold is kept securely.
- Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases.

Personal information should be:

- kept in a locked filing cabinet; or
- in a locked drawer; or
- if it is computerised, in a password protected file; or
- kept only on a floppy disk which is itself kept security.

Rights of access to information

Staff, students and other users of the University have the right to access any personal data that is being kept about them either on computer or in certain files. Any person who wishes to exercise this right should complete the University's *Access to Information* form and send or give it to the Data Protection Officer.

In order to gain access, any individual may wish to receive notification of the information currently being held. This notification is stored on the University's web site at <>

The University will make a charge of £10 of each occasion that access is requested under the Act, although the University shall have the discretion to waive this.

The University aims to comply with requests for access to personal information as quickly as possible but will ensure that it is provided within 21 days unless there is a good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request.

Publication of the University information

Information that is already in the public domain is exempt from the 1998 Act. It is the University policy to make as much information public as possible, and in particular the following information will be available to the public for inspection:

- names and contact details of University senior officers
- telephone and electronic mail directories of staff
- Degrees, diplomas and certificates of the University awarded to individuals
- Honorary awards of the University made to individuals

Any individual who has good reason for wishing details in these list all categories to remain confidential should contact the Data Processing Officer.

Subject Consent

In many cases, the University can only process personal data with the consent of the individual. In some cases, if the data is sensitive, express consent must be obtained. Agreement to the University processing some specified classes of personal data may be a condition of acceptance of a student to follow any scheme of study, and a condition of employment for staff. This includes information about previous criminal convictions.

The University may also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes.

The University will only use the information in the protection of the health and safety of the individual, but will need consent to process in the event of a medical emergency, for example.

Therefore, all prospective staff will be asked to sign a consent to process form, regarding particular types of information when an offer of employment is made. A refusal to sign such reform can result in the offer being withdrawn.

The Data Controller and Designated Data Controllers.

The University as a body corporate is the data controller under the Act, and the University is therefore ultimately responsible for implementation of the Act. However designated data controllers will deal with day to day matters.

Retention of data

The University will keep some forms of information for longer than others. Because of storage problems, information about students cannot be kept indefinitely, unless there are specific requests to do so. In general, paper-based information about students will be kept for a maximum of five years after they leave the University. This will include

- name and address
- academic achievements, including results and awards
- copies of any reference written
- details of any appeal.

All other information, including any information about health, race or disciplinary matters will be destroyed within three years of the student concluding his/her scheme of study (including any appeal) and leaving the University or three years of the award of his/her degree, diploma or certificate, whichever is the earlier.

The University will need to keep information about staff for longer periods of time. In general, information will be kept for three years after a member of staff leaves the University. Some information however will be kept for much longer. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references. A full list of information with retention periods is available from the Data Processing Officer.

Conclusion

Compliance with the 1998 act is the responsibility of all members of the University. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to University facilities is being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the Data Processing Officer.