

University of the West of England Data Protection Policy (FIN 022)

Introduction

The University needs to keep certain information about its employees, students and other users to allow it to monitor for example, performance, achievements, and health and safety. It is also necessary to process information so that;

- Staff can be recruited and paid
- Courses may be organised
- Legal obligations to funding bodies and government may be 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 that 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 that purpose.
- Be processed in accordance with the data subject's rights.
- Be kept safe from unauthorised access, accidental loss or destruction.
- Not be transferred to a country outside the European Economic Area, unless that 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 that this happens the University has developed the Data Protection Policy.

Status of the 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 rules and policies made by the University from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

Any member of staff, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the Assistant Vice-Chancellor Finance and Commercial Developments initially. If the matter is not resolved it may then 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 them and why.
- Know how to gain access to it.
- Know how to ensure it is kept up to date
- Know what the University is doing to comply with its obligations under the 1998 Act.

Responsibilities of Staff

All staff are responsible for:

- Checking that any information that 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 i.e. changes of address.
- Checking such information as the University may send out from time to time, giving details of information kept and processed about staff.
- Informing the University of any changes or errors of which they become aware. The University may not be held responsible for such errors unless the staff member informs the University of them.

If and when, as part of their responsibilities, staff collect information about other people, [including assessment of student work, opinions about ability, or details of personal circumstances], they must comply with the following data security requirements.

Data Security

All staff are responsible for ensuring that:

- Any 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, be password protected; or

- kept only on a disk which is itself kept securely.

Student Obligations

Students must ensure that all personal data provided to the University is accurate and up to date. In particular, they must ensure that changes of address, etc. are notified to the student registration office/other officer as appropriate.

Rights to Access Information

Any person who wishes to exercise their right to access information should complete the University access to information form. In order to help in deciding whether to request access, an individual may wish to request notification of the information currently being held. This application should be made in writing using the standard Data Protection Subject Access Request Form, obtainable from Financial Services (Ext 82607)

The University will make a charge of £10 on each occasion that access to information is requested.

The University aims to comply with requests for access to personal information as quickly as possible, and will ensure that it is provided within 40 days unless there is good reason for delay.

Publication of UWE 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 it judges to be appropriate. For example, the University's internal phone list will be a public document.

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 is a condition of enrolment of a student onto any programme, and a condition of employment for staff. This includes information about any criminal convictions.

Some jobs or programmes may bring an applicant into contact with children, including young people between the ages of 16 and 18. The University has a duty under the Children Act and other enactments to ensure that staff are suitable for the job, and students for the programmes offered. The University also has a duty of care to all staff and students and must therefore make sure that employees and those who use the University facilities do not pose a threat or danger to others.

The University may ask for information about particular health needs or problems, 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, and will need advance consent to use this information in the event of a medical emergency, for example.

All prospective staff will be required to sign a declaration on their contract of employment which provides consent to the recording and use of certain types of information.

The Data Controller and the Designated Data Controllers

The University is a body corporate and the ultimate data controller under the Act, and its Board of Governors is therefore ultimately responsible for implementation of this policy. It will be represented by the Assistant Vice-Chancellor Finance and Commercial Developments

(Corporation Secretary). However designated data controllers, one per Faculty\Service, will deal with day to day matters.

Assessment Information

Students will be entitled to information about assessment information and marks for both coursework and examinations, without charge. The University may withhold examination certificates, accreditation or references should an individual student have any outstanding financial obligations to the University.