DATA PROTECTION POLICY

1. Introduction

1.1 The University of Worcester is a data controller under the 1988 Data Protection Act ('the Act'). Its designated representatives for the purposes of information relating to students if the University Secretary and in relation to staff the Director of Personnel.

1.2 During the course of its business the University needs to process information about its employees, students and some other individuals. This information is processed in order to: monitor performance, achievements, health and safety, to ensure that staff are recruited and paid, courses are organised and legal obligations (e.g. to funding bodies and government) are fulfilled.

1.3 This information must be collected and used fairly, stored safely and not disclosed unlawfully. The University must comply with the Data Protection Principles in the Act. These state that personal data shall:

- Be obtained and processed fairly and lawfully and not be processed unless certain conditions are met;
- Be obtained for a specified and lawful purpose and not be processed in any manner incompatible with that purpose;
- Be adequate, relevant and not excessive for that purpose;
- Be accurate and kept up to date where necessary;
- 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 the country has equivalent levels of protection for personal data.

The University and all staff or others who process any personal information about other people on the University's behalf must ensure that they follow these principles at all times. The purpose of this Data Protection Policy is to ensure these principles are met.

2. Responsibilities of Staff

2.1 It is a condition of employment that employees will abide by the rules and policies of the University. Any failure to follow the institution's Data Protection Policy may therefore result in disciplinary proceedings.

2.2. 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 that they have provided about themselves e.g changes of address

2.3 If, as part of their responsibilities, staff collect or access information about other people (that is, personal data) they must comply with the University's Data Protection Policy; which is enshrined in the University's procedures for ethical approval of research projects.

2.4 Any member of staff who considers that the policy has not been followed in respect of personal information about themselves should first raise the matter with the Director of Personnel. If the matter is not resolved it should be raised as a formal grievance.

3. Responsibilities of Students

3.1 It is a condition of being a member of the University that students abide with the rules and policies of the University. Any failure to follow the institution's Data Protection Policy may therefore result in disciplinary proceedings.

3.2 All students are responsible for:

- Checking that any information that they provide to the University in connection with their membership of the University is accurate and up to date:
- Informing the University of any changes to information that they have provided about themselves e.g. changes of address

3.3. If, as part of their studies, students collect or access information about other people (that is, personal data) they must comply with the University's Data Protection Policy, which is enshrined in the University's procedures for ethical approval of research projects.

3.4 Any member of the student body who considers that the policy has not been followed in respect of personal information about themselves should first raise the matter with the University Secretary. If the matter is not resolved it should be raised as a formal grievance.

4. Data Security

4.1 All staff are responsible for ensuring that:

- Any personal information that they hold about other people is kept securely;
- Personal information about other people is not disclosed in any form to any unauthorised third party – this includes students' parents, partners, children and next of kin.

Unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct. Staff can incur criminal liability if they knowingly or recklessly

obtain and/or disclose personal information, without the consent of the University or the subject of the information. This means using information held by the University for their own purposes, which are outside the legitimate purposes of the University.

5. Rights of Data Subjects

5.1 All data subjects (e.g. the person the data is held about) are entitled:

- To know what information the University holds and processes about them and why:
- To gain access to it;
- To keep it up to date;
- In certain circumstances, data subjects are entitled to require the University to rectify, block, erase or destroy inaccurate information;
- To prevent processing likely to cause damage or distress;
- To prevent processing for the purposes of direct marketing (this may be particularly relevant to those with responsibilities for alumni or the recruitment of students)
- The right to compensation where a data subject suffers damage, or damage and distress, as a result of a breach of the Data Protection Act.

6. Rights to Access Information

6.1 Since October 2001 all individuals (data subjects) have had the right to access any personal information kept about them by the University, either on computer or in manual files.

6.2 Some information, such as student records, can be accessed automatically by the data subject. For information not automatically available, a subject access request may be made to the University Secretary and Pro Vice Chancellor (Students) using the University's Subject Access Request Form. The University may make a charge for providing the information, a charge or up to £1 is permitted for processing any request. The data subject should receive access to the information requested within 40 days of receipt of a written request, of if later, within 40 days of receipt of the fee, or any information necessary to satisfy the University as to the identity of the person making the request.

6.3 In instances where information about an individual is requested by a Police Authority they are required to make the request on an A222 form. The only time information should be released without the A222 form being provided in advance is in the case of emergencies, in cases where the information is required to protect the safety of either the data subject or others.

7. Publication of Information about the Institution

7.1 It is the University's policy to make public the following information:

- Certain information about members of the University's Board of Governors and senior management.
- Lists of staff

- The Institution's internal telephone and e-mail directory

7.2 Any person who has good reason for wishing details in these lists or categories to remain confidential should consult the University Secretary or Director of Personnel.

7.3 Staff may choose to withhold some personal information from the external telephone and email directory.

8. Subject Consent

8.1 In some cases the University may only process personal information with the consent of the subject; if the information is sensitive, explicit consent may be needed. It is a condition of registration of students and the employment of staff that they agree to the University's processing of specified classes of personal information. Guidance on handling sensitive data is contained in other University polices.

8.2 Sensitive data includes information about a person's racial or ethnic origin; political opinions; religious beliefs; membership of a trade union, physical or mental health; sexual life; criminal convictions or charges. The University processes some information that by this definition is classed as sensitive. Such information may be needed to ensure safety, to comply with the requirements of the government or of funding bodies, or to carry out institutional policies.

9. Examination Marks

9.1 Students will be entitled to information about their marks or grades for both coursework and examinations and this information is normally provided as a matter of course.

9.2 When a subject access request is made for examination marks or transcripts, the University is obliged to respond by the earlier of:

- 40 days after the announcement of the results or
- Five months from the receipt of the request, the fee and all reasonably required information.

9.3 If a student has not paid fees or charges or has not returned books or equipment, the University may withhold certificates, accreditation or references.

10. References

10.1 An individual may request access to any personal data held by the University and this includes personal references held on file for students and employees.

10.2 In the event of a request being made by any person for whom the University holds a reference, the permission of the person who provided the reference will be needed. All requests for references will be asked to consent to disclosure. Anyone refusing consent will be asked to state their reasons. If a referee declines consent a judgement will be made at the time of a subject access request on the available information. Efforts should be made to ensure anonymity.

10.3 Confidential references given by HE institutions are exempted from subject access requests and institutions have absolute discretion to refuse to release confidential references written on behalf of its employees or students. However, the University has decided that it will allow access to personal references held on file in the event of a subject access request by an employee or students.

11. Retention of Data

11.1 In general student files will be kept centrally for 10 years after they leave the University. Such files, paper and electronic, may contain academic or personal information. For historical purposes and to respond to authorised enquirers, the University keeps a record in perpetuity of past students and a summary of their academic record. Information held by departments may be held for shorter periods as appropriate.

11.2 In general all information about staff will be kept centrally in accordance with the University's Document Management Policy. 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.

11.3 The time limits for the retention of various forms of information can be found in the University's Document Retention Policy (http://www.worc.ac.uk/dpfoi/documents/RetentionSchedules.pdf).

12. Related Documents

- Data Protection Code of Conduct
- Freedom of Information Policy
- Information Security and Communication Policy

13. Conclusion

13.1 Compliance with the Data Protection Act 1988 is the responsibility of all members of the University. Breach of the Data Protection Policy may lead to disciplinary action or withdrawal of facilities. Any questions about the interpretation or operation of this policy should be referred to the Acting University Secretar.