DATA PROTECTION POLICY

1. INTRODUCTION

1.1 This policy document explains the framework through which the University ensures compliance with the Data Protection Act 1998 (DPA).

1.2 All personal data must be processed in accordance with this policy and DPA. Failure to comply may result in disciplinary action or even criminal proceedings.

2. SCOPE

2.1 The policy covers all processing of personal information as defined in the University's Data Protection Notification (Z6734933) to the Information Commissioner.

2.2 The policy applies to all staff, students, volunteers and contractors.

3. GOVERNANCE (Responsibility and Accountability)

3.1 The lines of responsibility and accountability for ensuring the University complies with DPA are as follows:

3.1.1 The Board of Governors is ultimately responsible for ensuring compliance.

3.1.2 The Secretary-Registrar is responsible for briefing the Board of Governors regarding compliance, annual renewal of the University's registration with the Information Commissioner's Office, managing data subject access requests, advising staff on data protection issues, and reviewing the data protection policy.

3.1.3 The Director of Human Resources is responsible for ensuring that appropriate training is available for members of staff and volunteers.

3.1.4 Deans of faculty and directors of service are responsible for ensuring that:

(a) all personal data within their areas are processed in accordance with DPA and university policy;

(b) a register of the paper and electronic systems (containing personal information) is maintained for their areas;

(c) personal data protection is audited annually and any subsequent action plans followed through appropriately.

3.1.5 All members of staff and students are obliged to comply with DPA (see sections 14 and 15 for details of staff and student obligations).

4. REGISTERS OF PERSONAL INFORMATION SYSTEMS

4.1 All faculties and service areas must create and maintain a complete register of their manual and electronic systems that contain personal data and information.

5. ANNUAL AUDIT OF PERSONAL DATA PROTECTION

5.1 An annual audit of personal data protection will be undertaken (at faculty/service area level) to ensure the University is in compliance with DPA. The audit is intended to:

5.1.1 raise general awareness of data protection;

5.1.2 demonstrate the University's commitment to data protection;

5.1.3 confirm that adequate controls exist;

5.1.4 identify any potential breaches of compliance;

5.1.5 verify that the university's personal data processing activities accord with the activities notified to the Information Commissioner's Office.

5.2 Departmental action plans will be produced to address any issues identified during audit.

6. PRIVACY IMPACT ASSESSMENTS

6.1 Where appropriate, for example where major changes are contemplated to systems or processes involving personal information, Privacy Impact Assessments (PIAs) may be used to identify potential issues and risks. Comprehensive information regarding PIAs is available at www.ico.gov.uk.

7. TRAINING

7.1 All staff and volunteers need to understand the importance of personal information processing and storage. Staff responsibilities will be explained to new members of staff during induction and appropriate additional training will be provided for employees who have responsibility for processing and/or management of personal data and/or information.

8. PRINCIPLES FOR PROCESSING PERSONAL DATA

8.1 The University has to comply with DPA's eight principles. This means that personal data must:

8.1.1 be obtained and processed fairly and lawfully and not be processed unless certain conditions are met;

8.1.2 be obtained for a specified and lawful purpose and not be processed in any manner incompatible with that purpose;

8.1.3 be adequate, relevant and not excessive for those purposes;

8.1.4 be accurate and kept up to date;

8.1.5 not be kept for longer than is necessary for that purpose;

8.1.6 be processed in accordance with the data subject's rights;

8.1.7 be kept safe from unauthorized access, accidental loss or destruction;

8.1.8 not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

8.2 The University will apply the above principles when processing personal data and meet all legal obligations to comply with DPA.

8.3 Staff or students who consider that the guidance or legislative requirements are not being followed in respect of personal data should raise the matter with the Head of Governance and Legal Affairs.

9. DEFINITIONS WITHIN DPA

9.1 The key DPA definitions are explained in sections 9.1.1 to 9.1.7 below.

9.1.1 DPA covers ***all*** personal data processed by the University, irrespective of whether these are held by individual members of staff in their own separate files (including those held outside the University campuses) or in departmental records systems or at the centre of the University.

9.1.2 Processing covers almost anything that is done to data, namely, collection, use storage and retention by reference to individuals

9.1.3 Personal Data is information about a living individual, who is identifiable by the information, or who could be identified by the information combined with other data, which the University has or may have in the future. This includes names and addresses, features such as hair and eye colour - which will often be in the form of photographs - student attendance records and marks, ethnic origin, qualifications and experience, details about staff sick and annual leave, dates of birth or marital status. Furthermore, any recorded opinion about or intentions regarding a person are also personal data; and this includes both student progress reports and staff review reports

9.1.4 Ordinary Personal Data includes name, address and telephone number.

9.1.5 Sensitive Personal Data including information relating to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life and criminal convictions. Under DPA the processing of sensitive data is subject to much stricter conditions. In particular, processing of sensitive data requires explicit consent. However, in most instances consent to process ordinary and sensitive data is obtained routinely by the University.

9.1.6 Data Subjects are the members of staff or students on whom information is held by the University.

9.1.7 Data Subject Requests can be submitted by data subjects in order to obtain copies of any personal information held by the University.

There is no entitlement to immediate or on-site access to information. HE Institutions normally have a maximum of 40 days in which to comply with a request for access by a data subject. [NB: This is 40 ordinary days, not working days].

10. ELECTRONIC DATA SYSTEMS

10.1 Electronically-held data encompasses not just the use of personal data held on databases but, for example, emails, letters and other documents held on disk or on hard drive.

11. MANUAL FILING SYSTEMS

11.1 Manual filing systems are covered by DPA. These may have the following characteristics:

11.1.1 grouping within common criteria, even if not physically kept in the same file or drawer;

11.1.2 structuring by reference to the individual by name, number, student cohort, degree scheme or other mechanism, or by criteria common to individuals, such as sickness, type of job, membership of pension scheme or department;

11.1.3 and, most pertinently of all, structuring that allows specific information about the individual to be readily accessible.

11.2 Data processors are advised to assume that all manual records concerning individuals will be caught by DPA.

12. SUBJECT CONSENT TO DATA PROCESSING

12.1 In many cases, the University can process personal data only with the consent of the individual. In some cases, if the data is sensitive, explicit consent must be obtained.

12.2 The University has a duty, under certain circumstances, to ensure that members of staff are suitable for the job, and students for the courses offered. On occasion, checks with the police or Criminal Records Bureau will be required to verify criminal records. (There are, for example, some jobs or courses that will bring the applicants into contact with children.) Where this is relevant to the job, the University may also ask for information about particular health circumstances. In such circumstances, the University will normally at the time of application advise applicants that they intend to seek such information and/or seek self-disclosure.

12.3 In most instances staff, (and where appropriate, students), will not need to obtain consent to process from data subjects because such consent is obtained routinely by the University. Upon student registration, students consent to processing a wide range of data. Staff will consent to do likewise on acceptance of an offer of employment. Agreement to the University processing this personal data is therefore a condition of acceptance of a student onto any course, and a condition of employment for staff. Refusal to provide consent may result in discontinuance of the application.

13. ACCESS TO DATA

13.1 Staff, students and others in contact with the University have, on most occasions, the right to access personal data that is being kept about them either on computer or in 'relevant' manual files. This will normally be provided in the form of copies of the personal data or a report of the data held, depending on the type and format of the original data. Any person who wishes to exercise this right should write to the Head of Governance and Legal Affairs. Data Access Request forms are available from the Registrar & Secretary's Office. The University will levy an administrative charge of £10 on each occasion that access is requested.

13.2 Where required to do so under DPA, the University aims to comply with requests for access to personal information from data subjects as quickly as possible, but will ensure that it is provided within 40 days from the date of the receipt of the request.

13.3 However, information about third parties must not be disclosed, unless they have given consent to disclosure. In the absence of consent, references to third parties should be deleted. Where this is not practical, access can be denied.

13.4 All enquiries from the police or other statutory agencies requesting access to data about individuals must be referred to the Head of Governance and Legal Affairs.

14. STAFF OBLIGATIONS

14.1 Many staff members have responsibilities for processing personal data about students (and in some instances, colleagues) as well as being data subjects in their own right. In connection with personal data on students and colleagues, all staff must comply with University guidelines on data protection. [*Guidance: what you need to know about the University's use of your personal information* is available as a separate document].

14.2 With regard to their own personal data, members of staff should:

14.2.1 ensure that any information they provide to the University, in connection with their employment, is accurate and up to date;

14.2.2 inform the University of any changes for which they are responsible, for example change of address. (The University cannot be held accountable for errors arising from changes about which it has not been informed.)

15. STUDENT OBLIGATIONS

15.1 Students are advised at registration about the information the University will collect, use and retain about them, and those to whom such information will be disclosed. Students must ensure that all personal data provided to the University are accurate and up to date. They must ensure that any changes, of address, for example, are notified to Planning & Registry Services, to their parent department and to other offices as appropriate. The University is not accountable for errors arising from changes of which it has not been informed.

15.2 Students who come into contact with personal data through the University for the purposes of research or study, in pursuit of an academic qualification and under the direct supervision of a member of staff will be covered by the University's notification to the Information Commissioner. In such cases, staff must notify students about, and students must abide by, the relevant provisions of this guidance. The University is not responsible for notification of personal data processed by students for their own use.

16. DATA SECURITY

16.1 All staff (and where appropriate, students) must ensure that:

16.1.1 any personal data which they hold are kept securely;

16.1.2 personal information is not disclosed either orally or in writing, intentionally or otherwise to any unauthorized third party.

16.2 Unauthorized disclosure of personal data will usually be a disciplinary matter and may be classified as gross misconduct.

16.3 Managers must ensure that, where a data processor processes data on the University's behalf (a mailing agency, for example), there is a written contract between the parties. The contract should specify that the processor agrees to act on the University's instructions and to abide by the provisions of DPA.

16.4 Staff should make reasonable efforts to ensure that all personal information is kept securely but should pay particular attention to the security of sensitive data. All personal data should be accessible only by those who need to use it and sensitive data must be:

16.4.1 kept in a lockable room with controlled access; or

16.4.2 kept in a locked filing cabinet; or

16.4.3 in a locked drawer; or

16.4.4 if computerized, be password protected; or

16.4.5 kept only on disks that are themselves kept securely.

16.5 While the security of the campus network is the responsibility of the University, individuals will need to take appropriate security precautions in respect of day-to-day PC usage. Care must be taken to ensure that PCs and terminals are not visible except to authorized staff and that computer passwords are kept confidential. Screens should not be left unattended when personal data is being processed and manual records should not be left where unauthorized staff can access them.

16.6 Off-site use of personal data presents a potentially greater risk of loss, theft or damage to personal data; and the institutional and personal liability that may accrue from the off-site use of personal data is similarly increased. Staff and students should take particular care when laptop computers or personal machines are used to process personal data at home or in other locations outside the University. Staff and students should also be aware that this

policy and their responsibilities under it apply when data are processed under such circumstances.

17. DISPOSAL AND DESTRUCTION OF PERSONAL DATA

17.1 It is not in the interest either of data subjects or the University to retain unnecessary or duplicative information. The University does, however, retain some data relating to former staff and students partly in order to comply with statutory requirements, and to maintain a complete historical record.

17.2 Documents containing personal data must be destroyed by shredding or incineration as soon as they reach their scheduled destruction dates. Redundant computer equipment must have personal data completely destroyed by either reformatting or overwriting hard drives.

18. SHORT-TERM AND VOLUNTARY STAFF

18.1 Managers who employ short-term staff and volunteers should ensure that any personal data is collected and/or processed in accordance with DPA. Managers must also ensure these people do not have access to personal data beyond what is essential for them to undertake their work.

19. VENDORS, CONTRACTORS, AND SUPPLIERS

19.1 Managers must ensure that vendors, contractors and suppliers are controlled, documented, required to wear some form of identification and sign non-disclosure agreements where access to personal data is unavoidable.

20. PUBLICATION OF UNIVERSITY INFORMATION

20.1 It is the University's policy to make as much information public as possible; in particular the following information may be available publicly (including on the University website):

20.1.1 lists of staff;

20.1.2 names and work contact information of staff;

20.1.3 University e-mail addresses;

20.1.4 photographs of staff;

20.1.5 student pass lists.

20.2 It is a condition of employment or registration that staff and students respectively consent to the processing of their personal data. It is recognized that there might be occasions when a member of staff or student has good reason for wishing details in certain of these lists or categories to remain confidential or to be restricted to internal access. In such cases, they should contact the Head of Governance and Legal Affairs for advice. In connection with the publication of photographic images of staff, particularly on web pages, all members of staff are advised that such images should not be made publicly accessible without the consent of the individuals concerned.

21. MONITORING OF COMMUNICATIONS AND USE OF CCTV

21.1 For reasons of personal security and to protect University premises and the property of students and staff, close circuit television cameras are in operation in certain campus locations. There are occasions when, to ensure the effectiveness of this surveillance, the presence of these cameras may not be obvious. The University has accordingly produced a policy on the use of CCTV cameras at the University.

21.2 In all instances:

21.2.1 monitoring will be carried out only by a limited number of staff;

21.2.2 personal data obtained during monitoring will be discarded as soon as possible after the investigation is complete; and

21.2.3 staff involved in monitoring will maintain confidentiality in respect of personal data.

21.3 Students or staff members who consider that the positioning of a close circuit television camera or use of a webcam is inappropriate should contact the Head of Governance and Legal Affairs.

22. WORLD WIDE WEB AND USE OF EMAIL

22.1 The University must ensure that its resources are not abused or used illegally, for example, for accessing pornographic material on the World Wide Web. In particular, both staff and students have responsibilities for using IT resources. The University may from time to time monitor staff and student communications without giving notice. Random monitoring of personal computer usage will apply only to publicly accessible computer clusters.

22.2 The provisions of DPA apply as much to web sites and to email as they do to data processing by any other means. Personal data downloaded from the web, included within a web site, or contained within an email are subject to the same restrictions as information held in manual files or on databases. In particular, authors of web pages should be aware that information posted onto a web page is potentially accessible worldwide (unless access is restricted in some way): the type of data placed onto web pages should reflect this.

22.3 The University has policies on the appropriate use of institutional IT facilities, and on the appropriate use of email and the web.

23. CROSS-BORDER DATA FLOWS

23.1 DPA places restrictions on the transfer of personal data outside the European Economic Area (EEA), unless the country or territory involved ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. If, after careful consideration, it is regarded as essential that the transfer of personal data outside the EEA should take place - and if the transfer does not qualify as one of the circumstances when this principle does not apply - the consent of

the data subject must be sought. Members of staff should note that this restriction has particular implications for international relationships, research projects and information placed onto web sites.

24. RESEARCH DATA

24.1 Personal data processed only for research purposes receive certain exemptions where the data are not processed to support measures or decisions with respect to individuals, and where no substantial harm or distress is caused. In essence, such personal data:

24.1.1 can be processed for purposes other than that for which they were originally obtained;

24.1.2 can be held indefinitely; and

24.1.3 are exempt from the data subject right of access where the data is processed for research purposes and the results are anonyms.

24.2 DPA does not give blanket exemption from all Data Protection Principles for data provided and/or used for research purposes. Most of the Principles apply (notably the requirement to keep data secure); and staff will need to assess the legality of processing on each occasion that data are provided for research purposes. Furthermore, researchers will need to ensure that:

24.2.1 data subjects whose personal data will be used in research are advised as to why the data are being collected and the purposes for which it will be used;

24.2.2 a suitable mechanism is in place to ensure that data subjects can meaningfully exercise their right to object to the processing of their data on the grounds that it would cause them significant damage or distress;

24.2.3 particular care is taken when the processing involves sensitive personal data for which stricter conditions apply, including the need to obtain explicit consent for processing.

24.3 Those conducting research involving the processing of personal data should do so in the context of any ethical guidelines or codes of practice particular to their field of study; and it may be necessary to confirm the compatibility of such codes with DPA.

25. CONFIDENTIAL REFERENCES

25.1 The University's position is to make clear that employment references are open. The position on academic references is less clear. For practical purposes staff must assume that we can neither guarantee confidentiality in respect of references received by the University nor expect that those we provide will remain confidential.

26. PROVISION OF REFERENCES OVERSEAS

26.1 Explicit consent must always be sought from the data subject where references are provided for organizations located outside the EEA.

27. EXAMINATIONS

27.1 Students will be entitled to information about examination marks. However, the University has a longer period to respond to access requests (40 days from the announcement of the results, or five months from the date of the request). The University may withhold awards, certificates, accreditation and references in the event that full course fees have not been paid, or books and equipment not returned, but may not withhold marks for these reasons.

27.2 Internal and external examiner comments, whether made on the script or in another form that allows them to be held and applied to the original script or to a specific candidate (e.g. an examiner's report) are covered by DPA. A data subject has the right to request that a copy or summary of such data be provided within the stipulated timescale 'in an intelligible form'. This implies that any examiners' comments written on scripts and assessed work should be capable of being produced for a data subject in a meaningful form and that they should be both intelligible and appropriate. Minutes and other records that identify individuals will also be accessible.

28. DISCIPLINE

28.1 Any breach of this policy or DPA may lead to disciplinary action under the applicable staff or student procedure or even criminal prosecution.

29. POLICY REVIEW

29.1 This policy will be reviewed on a rolling three-year basis, or sooner if necessary to ensure compliance with any changes to DPA.

30. FURTHER INFORMATION

30.1 This policy document is not an authoritative statement of the law.

30.2 If you have any queries, or require further advice, please contact the Head of Governance and Legal Affairs.

30.3 The Joint Information Systems Committee (JISC), acting for the sector, has produced a data protection code of practice for higher and further education institutions. This is available online at:

http://www.jisc.ac.uk/publications/publications/pubdpacop0101.aspx.

30.4 This policy should be read and understood alongside University documentation in respect of the Freedom of Information Act 2000.

This policy was approved by the Board of Governors by resolution 275.2011.HEC of 20 July 2012 with effect from 01 August 2015 and is due for review no later than 31 July 2016.