University for the Creative Arts

Data Protection Policy and Procedures

1. The Data Protection Act 1998

1.1 The Data Protection Act of 1998 ("the DPA") gives rights to individuals to access 'personal data' (being information which identifies and relates to a living individual, either on its own or when combined with other information held by the University or on its behalf) about them that is collected and 'processed' (see 2 below). It includes all personal data that is held automatically including word processed documents, in databases and e-mails and personal data held in manual records where these can be accessed by reference to a person or otherwise located with assistance from the individual. As the University is a public authority and subject to the Freedom of Information Act, 2000, the definition of personal data also comprises any personal data that is not held electronically and is held in an unstructured manner by the University. The University has to comply with the requirements of the DPA in respect of the information it holds about its students and staff and other individuals. It is the responsibility of all members of the University to ensure compliance with the DPA when they deal with personal data.

1.2 The DPA requires the University to notify the Information Commissioner, (the regulator responsible for enforcement of the rights and obligations set out in the DPA) of the types of personal data that it holds, the categories of individuals for which it holds this information, to whom it may be disclosed and the purposes for which personal data is processed ("the Notification"). It also requires the University to confirm if it transfers personal data outside of Europe.

1.3 The Policy and Procedures set out how the University will comply with the requirements of the DPA. They will not be incorporated into contracts of employment. Additional guidelines will be available for staff.

2. Data Processing

2.1 "Processing" of personal data within this policy means the obtaining, recording, storing or holding of personal data. It also includes the carrying out of any operation using that personal data such as altering or deleting it, consulting it or disclosing it. The University and all of its staff must ensure that all processing of personal data carried out by the University is in accordance with the requirements of the DPA, in particular that:

- all personal data must be processed fairly and lawfully;
- personal data shall be obtained only for one or more specified and lawful purpose(s);

- personal data shall be adequate, relevant and not excessive;

personal data shall be accurate and, where necessary, kept up to date;

- personal data shall not be retained for longer than is necessary for those purpose(s);

- personal data shall be processed in accordance with the rights of data subjects under the DPA;

- appropriate security measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data; and

- personal data shall not be transferred to a country outside the European Economic Area unless an adequate level of protection is in place.

2.2 The Data Protection Officer will be responsible for notifying the Information Commissioner of any data processing carried out by the University and for ensuring that the Notification is kept up-to-date and reviewed and renewed annually. Two or more Data Control Officers will be responsible for supervising data control and for assisting those processing personal data to comply with this policy. The names of the Data Control Officer(s) are recorded in Appendix One.

2.3 It is the responsibility of any member of staff who has access to and processes personal data to ensure that he/she complies with this policy, is familiar with the University's Notification to the Information Commissioner and processes personal data in compliance with that Notification. Staff can consult the Notification on the Information Commissioner's Web site http://www.ico.gov.uk)
Further information and guidance on any aspect of this policy or details of the Notification may be obtained from the Data Control Officer(s).

2.4 If you become aware of any new or different use of personal data, or wish to collect additional personal data, or to use it in a new way, you must inform the Data Protection Officer in writing as soon as possible for them to assess whether or not such change will comply with the DPA and, if it does, so they may update the Notification in advance of such change or otherwise as soon as possible.

2.5 Employees should not use University facilities to process personal data for purposes unconnected with their employment or for domestic or personal purposes. Such processing is not covered by the University Notification.

2.6 If the University receives any written or electronic correspondence from:

2.6.1 the Information Commissioner's Office relating to the University's data processing activities;

2.6.2 any individual looking to exercise his/her rights under the DPA;

2.6.3 any individual wishing to complain about the University's processing of his/her personal data

Such correspondence must be passed to the Data Protection Officer as soon as possible and without delay.

3 Data Collection

3.1 Data relating to the University's employees, organisation structure, students and other individuals with a relationship to the University (e.g. suppliers, landlords, enquirers, alumni) is collected and processed by the University for it to comply with its legal obligations and duties, exercise its rights and powers and by doing so to operate the University as intended. Such processing includes use to specifically provide:

3.1.1 information, whenever required, for planning and managing the University's activities including:

3.1.2 information, whenever required, for planning, delivering and monitoring the University's portfolio of courses;

3.1.3 information for the purposes of research and private study and links with business and the community;

3.1.4. individual information for managing the employment, deployment and welfare of individual employees;

3.1.5 individual information for managing the attendance, performance and welfare of individual students;

3.1.6 information, whenever required, for responding to legitimate external enquiries about the University's students and/or employees;

3.1.7 assistance with human resources and salary administration procedures, e.g. payroll; and with procedures relating to the collection of student fees.

3.2 The Data Control Officer(s) shall review annually:

3.2.1 the nature of information being collated or held to ensure there is a sound business reason for doing so;

3.2.2 the length of time personal data is being held and whether this complies with clause 2.1.5;

3.2.3 whether personal data that is no longer required is being securely deleted;

and determine (with assistance from the appropriate University departments if necessary) that such use is compliant with the DPA.

3.3 Wherever possible, to the extent required by the DPA, employees/students, potential employees/students or third parties will be advised of what personal data is obtained or retained, its source, and the purposes for which the personal data may be used or disclosed. Consent will be sought mainly by way of general consent at the point at which the

information is collected. In the case of sensitive personal data[1] the individual will be asked for his/her explicit consent to that personal data being processed where legally required.

3.4 Initial personal data is ordinarily obtained from job or course application forms submitted to the University and thereafter principally from employees and students themselves. Job and course application forms will clearly state the purposes for which information will be used and personal data will only be used in accordance with such information or where legally required or lawfully permitted under the DPA.

3.5 Employees/students should not be induced to provide information or be led to believe that a failure to supply information requested by the University might disadvantage them where this cannot be justified.

3.6 Permission should be sought from individuals about whom any personal data relates prior to any automated decisions being made about them using that personal data. Individuals have special rights in such cases, including a right to request such decisions be made manually.

3.7 Wherever new personal data is to be collected, it is the responsibility of the University (and those acting on its behalf) to ensure that it only uses personal data for the purpose(s) for which such data was collected by the University. Proposed changes of use will normally need to be notified to the affected individuals and their consent to such new or varied use may be needed.

4 Disclosure of Data

4.1 To ensure compliance with the DPA and in the interests of privacy, employee/student confidence and good employee/student relations, the disclosure and usage of information held by the University is governed by the following conditions:

4.1.1 Save for statutory compliance or as permitted by the DPA, it must only be used for one or more of the purposes specified in the Notification to the Information Commissioner and as notified to or reasonably expected by the relevant individuals.

4.1.2 Provided that the identification of individual employees/students is not disclosed, aggregate or statistical information may be used in accordance with the Information Commissioner's Code on Anonymisation to respond to any legitimate internal or external requests for personal data, e.g. HEFCE returns, workplace surveys, market research, academic research (see also paragraph 12). It must be made clear to individuals in advance how their details may be anonymised and what the anonymised details would be used for.

---

[1] Sensitive personal data for this purpose includes information relating to an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual orientation or the commission or alleged commission of offences. In the latter case this may include any proceedings for any offence committed or alleged to have been committed by the individual, the disposal of such proceedings or the sentence of any court.

4.1.3 Personal data must not be disclosed, either within or outside the University, to any recipient who is not authorised in the terms of the DPA, or for any purpose which is not authorised by the University's Notification. All disclosures must be proportionate, secure and on a need to know basis. Disclosures to outside the University can only be made if permitted by the DPA, such as where necessary to perform a contract with the individual concerned, or where necessary to meet the legitimate interests of the University or intended recipient (provided always that there is no unwarranted prejudice to any affected individual). Special care is needed for details whose loss or misuse may cause damage or distress (such as financial or identification details which could be used in fraud or identity theft). Even more care is needed to disclose sensitive personal data, such as health details. Normally individual consent will be needed and the details should be encrypted before being sent electronically as the disclosure must be secure.

4.1.4 Members of staff processing personal data should seek guidance from the Data Control Officer(s) if any doubt surrounds a request for personal data, whether internal or external. Even where an individual requests their own personal data, you must be certain you are dealing with that individual (or someone properly authorised to act for them and have evidence of that). Unless essential to comply with a court order or statutory provision, all disclosures of personal data by the University are voluntary and at its risk. Where a request is from a third party, such as the police or a government department, the University must have an audit trail to show any disclosure was fair, lawful and justified under the DPA, as well as being proportionate to need. Personal data must not be provided to third parties verbally without specific prior authorisation from the Data Protection Officer. Many security breaches are by 'blagging' where a third party tricks an employee into giving them personal data without any authorisation or legal justification.

NB. External requests for information should be made in writing and members of staff should be satisfied about the legitimacy of requests for information and seek valid documentary evidence. In the case of a request by an individual for their own personal data, the permitted £10 fee may be requested if appropriate (see below).

4.2 Requests for personal data by external recipients of data, which **do not** require the consent of the data subject (but which must still be assessed to ensure they are valid and lawful and justified) are:

4.2.1 requests made for the purposes of law enforcement (i.e. for the prevention or detection of crime, the assessment or collection of any tax or duty or the assessment or collection of any liability via the Child Support Agency). Disclosure is only allowed where failure to make disclosure would be likely to prejudice one of those purposes. In all cases written evidence must be obtained from the Police, Inland Revenue, Customs and Excise and the Child Support Agency (as appropriate) as to the purpose of the request.

4.2.2 requests in relation to any other compulsory legal processes; again, appropriate written evidence must be obtained beforehand.

4.1.3 requests, if urgently required, for the prevention of injury and damage to health. If needed to protect the vital interests of the employee/student, disclosure may be made without prior consent. Otherwise, the written consent of the employee/student must be obtained beforehand.

4.1.4 requests made by pension administrators, in order to administer the University's participation in various external pension schemes.

4.3 Examples of requests for personal data by third parties, which **do** require the consent of the data subject are:

4.3.1 requests from agents authorised by the employee/student who is the subject of the personal data, for e.g. mortgage requests, references. Confirmation should be sought from the employee/student, that the information is to be released and, normally the employee/student's written consent should be obtained.

4.3.2 requests required by authorised officials or representatives of recognised trade unions. Confirmation should be sought from the employee, that the information is to be released and, if possible, the employee's written consent should be obtained.

NB. All staff should endeavour to restrict disclosures requested from outside of the University to those required by law as much as possible and should, at all times follow the University's security requirements detailed in section 7.

5 Accuracy of Data

5.1 Updating is required only "where necessary" on the basis that, provided the University has taken reasonable steps to ensure accuracy (e.g. asking the individual to provide accurate details, or to update them at regular intervals, or taking up references), personal data held is presumed accurate at the time it was collated. The University must ensure details it inputs are accurate and are held in records in a consistent manner.

5.2 All employees/students should be made aware in writing of the importance of providing the University promptly with notice of any change in personal circumstances and details.

5.3 Employees/students will be requested to update personal data on an annual basis for the purposes of ensuring that the data is up-to-date and accurate. Employees/students may be entitled to correct any details although in some cases the University may require documentary evidence before effecting the correction, e.g. by seeking examination/qualification certificates for amending qualification details. The University is not obliged to make all changes or corrections requested if it believes that the request is unreasonable eg it could lead to an inaccurate record of events. In such cases, please liaise with Data Protection Officer for assistance (please see below).

6 Employees'/Students' Rights

6.1 Employees/students are, at reasonable intervals (which the University deems to be every six months) entitled to have access to personal data held upon them which is not excluded personal data (see paragraph 6.9 below) (a subject access request, or SAR). A fee (£10) may be levied for this service (see paragraph 6.8 below). They are also entitled to ask for and be informed of the purpose(s) for which the personal data is or is intended to be used, its source(s) and the likely recipient(s) (or classes of recipient)

6.2 Students are, in addition, entitled to access their own assessment results and this information will normally be supplied routinely. Assessment submissions are expressly exempted from data subject access rules. This means that the University is under no obligation to permit candidates to have access either to original scripts or to copies.

6.3 Assessors' comments, whether made on the assessed submission or in another form that allows them to be held and applied to the original script are not exempt. Staff should ensure that comments are capable of being reproduced for a student in a meaningful form on an assessment feedback form.

6.4 Students will have access to minutes of assessment boards that contain discussion about them where candidates are referred to by identifiers from which they may be identified, unless that personal data cannot be disclosed without additionally disclosing personal data about a third party which it would not be reasonable to disclose.

6.5 Assessment results may be disclosed to third parties on notice boards specified for the purpose. Identifiers rather than names must be used and students should be given an explanation in advance of where and how they should expect their results to be posted. Students should be given the right to object to their results being displayed if such disclosure will cause them damage – for example if their whereabouts would be made known and this would put them at risk.

6.6 Assessment results must not be given over the phone.

6.7 The University will comply with a request from a student to supply a record of his or her assessment results or comments either five months from the date of the request or forty days from the date on which the results were first announced, whichever is earlier.

6.8 The recipient of a subject access request from an employee/student must immediately refer it to the relevant Data Control Officer. The request must be in writing and the Data Control Officer must respond promptly on behalf of the University and in any event before the end of 40 days from the date on which the request was first received (subject to paragraph 6.7). This is however, conditional upon the Data Control Officer being provided with sufficient information to identify the relevant employee/student and, where the personal data is unstructured, to locate that unstructured information. The University is allowed to charge a fee for providing this information of up to £10 for each request. In the case of current employees the University will waive this charge for the time being. In the case of current students, the University reserves the right to charge a fee of £10, depending on the extent of the personal data requested. In

using its discretion, the University will not be unreasonable. Access to records such as an enrolment form, assessment results, a student transcript will not command a fee.

6.9 Certain personal data is excluded from the obligation to supply it in response to a subject access request and will not be provided in response to a disclosure request. These include:

6.9.1 confidential references given by the University when these relate to the education, training or employment of staff or students;

6.9.2 personal data processed for the purposes of management forecasting or management planning to the extent that disclosure would be likely to prejudice the conduct of that business or activity only;

6.9.3 personal data which consists of records of the intentions of the University relating to any negotiations with the employee/student to the extent that disclosure would be likely to prejudice those negotiations only;

6.9.4 if, in order to comply with a disclosure request, the University would need to disclose information relating to an identifiable third party then disclosure is not required unless the third party consents or it is otherwise reasonable to comply with the request without such third party consent. If the information sought is a health record and the third party concerned is a health professional who has compiled or contributed to that health record or has been involved in the care of the data subject in his capacity as a health professional then disclosure should be made.

6.10 In addition to seeking disclosure of information, an employee/student is also entitled to request that the University does not process data concerning him/her where this will cause or be likely to cause substantial and unwarranted damage or distress, either to the employee/student concerned or to a third party. Such a request will need to be submitted in writing and, where possible, will be agreed by the University. Upon receipt of a written request from an employee a Data Control Officer will write to the employee/student within 21 days confirming that the request will be upheld or giving reasons why it will not.

6.11 The employee/student will not be able to prevent processing if the processing is necessary for compliance with any legal obligation or it is necessary to protect the vital interests of the employee/student or it is necessary for the performance of a contract to which the employee/student is a party.

6.12 An employee/student who feels that he/she has, or is likely to suffer damage as a result of either inaccuracy in the personal data held by the University or as a result of unauthorised disclosure of information must notify a member of the Human Resources Department/Academic Registry in writing immediately. Where appropriate, the University will correct or erase that information or indicate that the information is contested by the employee/student.

6.13 In the event of a complaint in relation to this policy, students should use the official Complaints Procedure published in their course handbooks, whilst employees should use the Grievance Procedure.

6.14 In some cases personal data is held by the Student Union or student societies within the Union. The University looks upon the Student Union as an autonomous body and in such capacity the University expects the Student Union to be responsible for the notification of personal data to the Information Commissioner. The Data Controller will liaise with a member of the Student Union to try to ensure that personal data is properly notified.

7 Security

7.1 This policy should be read in conjunction with the Information Security Policy and Records Management Policy.

7.2 In order to prevent unauthorized disclosure of or access to personal data, the following security measures will be required in respect of the processing of any personal data:

7.2.1 Access to personal data on staff and students is restricted to those members of staff who have a legitimate need to access such data in accordance with the University's Notification.

7.2.2 Members of staff authorized to access personal data under paragraph 7.2.1 above, will be allowed to do so, only in so far as they have a legitimate need and only for the purposes recorded in the Notification.

7.2.3 All persons processing personal data and individuals requesting access to personal data in accordance with this policy must have familiarised themselves with this policy and the Information Security Policy and it will be the task of the Data Control Officers to ensure that all such personnel are thoroughly trained in their use.

7.2.4 Access to computer held electronic personal data is subject to the same restrictions as above save that all staff authorised to access personal data will be required to have passwords in order to access the data. These passwords will be changed at regular intervals to ensure security is maintained. **Disclosure of a password to any other employee will result in a formal disciplinary investigation.**

7.2.5 All personal data will be stored in such a way that access is only permitted by authorised staff. This includes personal data stored in filing cabinets and other storage systems. **Acts or omissions by employees which lead to unauthorised access or disclosure will lead to a formal disciplinary investigation**.

7.2.6 Personal data should be transferred under conditions of security commensurate with the anticipated risks and appropriate to the type of personal or sensitive personal data held. Sensitive personal data (or data whose misuse or loss may cause substantial damage or distress) must not be emailed unless encrypted. It should not be emailed to 'distribution list' emails without prior written authorisation from a Data Control officer. Wherever possible do not email attachments containing personal data, especially sensitive personal data. Instead, wherever

possible require people to access the personal data in secure systems, using their authorised access details.

7.2.7 Personal data held electronically must be appropriately protected, backed up and stored securely to avoid incurring liability to individuals who may suffer damage or distress as a result of the loss or destruction of their personal data.

7.2.8 Any disposal of personal data will be conducted in a secure way, normally by shredding or security waste. All computer equipment or media to be sold or scrapped must have had all personal data completely destroyed, by re-formatting, over-writing or degaussing.

8 Third Parties

8.1 Any personal data which the University receives and processes in relation to third parties, such as visiting academics, suppliers, landlords, employers, alumni, enquirers and other individuals on mailing lists etc. will be obtained lawfully and fairly and dealt with in accordance with the principles and conditions of the DPA.

8.2 Members of staff should ensure that in all cases the use to which the personal data is to be put is registered in the Notification (See 4.4).

8.3 Where proposed use of personal data extends beyond the necessary use of it in the context of the relevant relationship, or the reasonable expectations of the individual concerned, members of staff should obtain explicit consent from third party personal data subjects to process such personal data for the purposes expressed in the Notification and should ensure that there is a mechanism for:

8.3.1 dealing with any data subject access requests made by third parties;

8.3.2 allowing third parties to withdraw consent to the processing of their personal data for the purposes of direct marketing; and

8.3.3 allowing third parties to object to the disclosure of their personal data.

9 Transfer of Data outside the UK

9.1 It is a requirement of the DPA that personal data shall not be transferred to any country or territory outside of 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. 'Transfer' for this purpose includes personal data being physically or electronically sent, being located on a server abroad, or even if on a sever in Europe, being remotely accessed from abroad.

9.2 For the avoidance of doubt the European Economic Area currently includes Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia,

Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and UK.

9.3 The University may allow information to be transferred outside of the EEA where the recipient has been deemed by the EU Commission to offer adequate safeguard for personal data, such as Switzerland.

9.4 The University may also transfer personal data outside the EEA to a recipient:

9.4.1 in the US and which has a current and suitable safe harbor certification covering the personal data to be transferred; or

9.4.2 outside the EEA who has entered into the relevant form of the European Commission approved model data transfer terms with the University; or

9.4.3 who has other arrangements which provide adequate safeguard for the personal data, as recognised by the Information Commissioner. Please liaise with Data Protection Officer for any queries about such arrangements.

9.5 There are specific exceptions to the general rule which may allow information to be transferred outside the EEA. These should only be used where the above options are not feasible and with the prior consent of Data Protection Officer. The University needs to be able to justify and evidence its reasons for transferring personal data if using these criteria for transfers outside the EEA. The exceptions where details may be exported where necessary can be summarised as follows:

9.5.1 with consent: (the University will seek the explicit consent of a student/employee if it becomes necessary to process and transfer personal data);

9.5.2 to make or perform a contract;

9.5.3 in legal proceedings;

9.5.4 to protect the vital interests of the individual;

9.5.5 for substantial public interest;

9.5.6 where the information is on the public register;

9.5.7 on terms approved by the Information Commissioner or where authorised by the Information Commissioner.

10 Student use of Personal Data

10.1 Members of staff directly supervising students (normally research students) who are processing personal data for the purposes of research or study or in pursuit of an academic qualification should ensure that the personal data being processed is adequately covered by the University's Notification. Awareness of the need to comply with this policy should be promoted to students through publications such as the 'Dissertation Guidelines'.

10.2 Where students process personal data for the purposes of research or study or in pursuit of an academic qualification, but not under the direct supervision of a member of staff, (normally FE, BA and PG students) such processing will be deemed to be for the students' own personal or domestic purposes and the processing will be exempt from notification by the University.

11 Contractors and Suppliers

11.1 In certain circumstances it may be necessary to allow contractors or suppliers access to personal data in the course of maintenance or repair work.

11.2 In such circumstances, contractors should be documented and wear some form of identification. They should be restricted from unnecessary admittance to areas where personal data is held or processed and, if necessary, required to sign nondisclosure agreements, if access to personal data is unavoidable.

11.3 The University is obliged to put 'appropriate technical and organisational' security measures into place, as part of complying with this obligation, if the University decides to appoint a third party data processor to process personal data on its behalf then:

11.3.1 the University must enter into a written contract with the data processor to confirm the third party's appointment as data processor;

11.3.2 the contract must state that the data processor will only use the personal data in accordance with the University's instructions; and

11.3.3 the contract must state that the data processor is to keep the personal data secure in accordance with its obligations under the Seventh Data Principle under the DPA.

11.4 In addition, it is best practice (and the Information Commissioner would expect) additional commercial restrictions relating to audit enforcement and security breach to be in place. You must liaise with the Data Control Officer before authorising any contractor or supplier to collect or use personal data for the University (or to supply personal data to the University) to enable the Data Control Officer to ensure that the arrangement complies with the DPA and that any necessary contractual terms are in place.

12 Staff use of personal data off-site, on home computers or at remote sites

12.1 Employees processing personal data off-site should comply with the obligations set out in the University's Information Handling Policy and the University's Information Security: mobile working and remote access policy and other relevant policies, in particular with regard to obtaining the necessary authorisations

12.2 Employees should at all times:

12.2.1 attempt to minimise the amount of personal data that is processed off-site;

12.2.2 keep a record of all personal data taken off-site and when it was returned;

12.2.3 never leave the personal data unsupervised or unsecured;

12.2.4 ensure they take reasonable precautions to prevent the personal data from being accessed, disclosed or destroyed as a result of any act or omission on their part.

12.2.5 notify the Data Protection Officer immediately in the event of any loss, damage, unauthorised access or theft thereof.

13 Use of Personal Data in Research

13.1 The DPA provides certain exemptions for 'research purposes' including statistical or historical purposes.

13.2 Provided that the purpose of research processing undertaken by staff and students is not measures or decisions targeted at particular individuals and it does not cause substantial distress or damage to a data subject, then personal data may be:

13.2.1 processed for purposes other than for which they were originally obtained;

13.2.2 held indefinitely;

13.2.3 exempt from the right of access by data subjects where the results do not identify data subjects.

13.3 Most of the Data Protection Principles (set out in Schedule 1 of the DPA, see section 2 above) still apply to personal data used for research purposes and researchers should always provide clear guidance to individuals whose personal data will be used in research as to why the personal data is being collected, how it will be anonymised and the purposes for which it will be used, including any potential consequences for that individual.

14 Collection of Personal Data from Web Pages

14.1 The University will provide the following information on any Web pages designed to collect personal data:

- The identity of the University as the responsible data controller under the DPA;

- the purpose(s) for which the personal data is being collected;

- the recipients or classes of recipients to whom the personal data may be disclosed;

- an indication of the period for which the personal data will be kept;

- any other information to ensure that the processing is within the 'reasonable expectations' of the individual data subject.

14.2 The University will provide users with the opportunity to opt out of any parts of the collection of or use of the personal data that are not directly relevant to the intended transaction.

14.3 If cookies are used at any time on a University website, additional information on the type, proposed owner / data controller of all such cookies must be provided in accordance with the Privacy and Electronic Communication Regulations 2003. Please liaise with the Data Protection Officer for more details.

15 **Marketing**

15.1 Special rules apply to marketing communications, especially by electronic means, such as email. If you wish to send any marketing communications, please liaise with the Data Control officers before doing so to ensure such use complies with the DPA.

16 Contractors, Consultants and Service Providers

16.1 The University expects the highest standards of compliance from its contractors, consultants and service providers. The obligations on and expectations of staff in this policy, apply equally to contractors, consultants and service providers using University personal data.

APPENDIX ONE: DATA CONTROL OFFICERS

Data Protection Officer	Marion Wilks, University Secretary & Clerk to the Board of Governors
Responsibility:	Data Protection Policy Notification Advising on policies relating to third parties
Data Control Officers	Angela Fisher, Director of Human Resources
Responsibility:	Advising on policies relating to staff data
	David Burt, Academic Registrar
Responsibility:	Advising on policies relating to student data