Data Protection Policy

Approved by:	Board of Governors
Date last approved:	1 October 2019
Review period:	3 years
Date of next review:	1 October 2022
Owner:	University Solicitor

University for the Creative Arts

Data Protection Policy and Procedures

This Data Protection Policy ("Policy") regulates the way in which the University for the Creative Arts ("the University") obtains, uses, holds, transfers and otherwise processes Personal Data about individuals and ensures all of its employees and students know the rules for protecting Personal Data (as defined below). Further, it describes individuals' rights in relation to their Personal Data processed by the University.

The University has practices in place in relation to its handling of personal information to ensure that the University and its employees are acting in accordance with UK laws and regulatory guidance. These practices, together with this Policy, and the Information Security policy, ensure that all employees of the University fully understand the University's obligation to abide by the data privacy laws and regulations of the UK.

The obligations on and expectations set out in this Policy, apply equally to all permanent, sessional and temporary staff, contractors, consultants, agents, service providers and students ("you").

1. What is Personal Data?

1.1 "Personal Data" is any information (for example, a person's name) or combination of information about a living person which allows that living person to be identified from that information (for example a first name and an address). Examples of Personal Data which may be used by the University in its day-to-day business include names, email and land addresses, telephone numbers and other contact details, CVs, performance reviews, payroll and salary information.

1.2 It also includes records of behaviour of individuals, any expression of opinion about individuals and any indication of intentions in respect of individuals.

1.3 When considering whether data allows a person to be identified, you must consider it as a jigsaw piece and whether, with all the other jigsaw pieces the University holds in respect of that person, when put together they would enable identification of that person.

1.4 The laws governing the use Personal Data apply whether the Personal Data is stored electronically (for example, in emails, on IT systems, as part of a database or in a word-processed document) or in structured paper records (for example, in paper files, card indexes or filing cabinets).

1.5 You also need to take special care of other Personal Data where it should be clear its loss or misuse would be likely to place individuals at greater risk, or cause them distress, such as very private information, details about bank accounts or credit cards, and information which could be used for fraud or identity theft, such as passport or national insurance number details.

2. Why is Data Protection legislation important to the University?

2.1 The University has to comply with the requirements of the data protection and related ePrivacy laws in respect of the Personal Data it holds about its students,

staff and other individuals. It is your responsibility to ensure compliance with the data protection legislation when you deal with Personal Data.

2.2 The key data protection laws which apply to the University are the Data Protection Act 2018 ("DPA") and the General Data Protection Regulation ("GDPR"), together with the Privacy in Electronic Communications (EC Directive) Regulations 2003 ("PECR"), which will, eventually be replaced by the Privacy in Electronic Communications Regulation ("EPR").

2.3 The GDPR updates and upgrades data protection laws and the University depends on you to help it comply with its obligations. It will be important to ensure that you are aware of and comply with all relevant University policies and procedures and attend any training provided.

2.4 Data protection laws are enforced in the UK by the Information Commissioner's Office ("the ICO"). The ICO can investigate complaints, audit the University's use of Personal Data and can take action against the University (and you personally in some cases) for breach of these laws. The impact on individuals of any breach must not be forgotten or underestimated, as it may involve intrusion, distress, identity theft, fraud and financial loss. Action may include making the University pay a substantial fine and/or stopping the use by the University of the Personal Data, which may prevent the University carrying on its business. Institutions who breach one or more laws in respect of the processing of Personal Data also often receive negative publicity for the breaches which could affect the reputation of the University and its business as a result.

2.5 It is a legal requirement for the University to register with the Information Commissioner's Office as the supervisory authority. The University's registration number is Z6218018 and is renewed annually.

2.6 The Policy explains how the University will comply with the requirements of the data protection legislation. Each University staff member, students, consultant, agent, contractors and service providers is required to read and comply at all times with this Policy. The Policy will not be incorporated into contracts of employment.

2.7 Please read this Policy carefully and if you have any queries, contact the Data Control Officers or the Data Protection Officer listed in Appendix 1.

3. What activities are regulated by this Policy?

3.1 The University processes Personal Data (including Sensitive Personal Data, see below for more information) on its employees, contractors, students, business contacts, customers, suppliers and any other individuals, including job applicants and former employees and students, depending on the relationship with them, for a multitude of business purposes, including:

- education and support services to students and staff, including the administration of accommodation and tuition fees;
- advertising and promoting the University and the services we offer;
- alumni relations;
- production of university publications;

- research and development and fundraising;
- managing our accounts and records and providing commercial activities to our clients;
- personnel record keeping and management;
- employee performance management and professional development;
- employee benefits and succession planning;
- payroll and pensions, including returns, fund management and accounting;
- contract performance, including buying and selling goods and services;
- recruitment;
- business and market development;
- building and managing external relationships;
- work and business project scheduling;
- knowledge management;
- compliance programs and policies; and
- other purposes required by law or regulation or notified to you under separate policy documentation from time to time.

3.2 When you collect, record, organise, structure, store, adapt, alter, retrieve, consult, use, disclose by transmission, disseminate or otherwise make available, update, erase or destroy Personal Data for any of these purposes, this is called "Processing". If you make use of Personal Data (e.g. read, amend, copy, print, delete or share Personal Data, whether within the University or outside of the University) this is also a type of processing and is subject to the guidelines set out in this Policy.

4. Data Processing

4.1 Use of Personal Data held by the University is governed by the following rules in order to ensure compliance with the data protection legislation and in the interests of privacy, employee and student confidence and good employee and student relations. The University adopts a privacy by design and default approach to its collection and use of Personal data which all of its staff must comply with.

4.2 The University must ensure that all processing of Personal Data carried out by the University is in accordance with the Data Protection Principles and other obligations set out in the data protection legislation, in particular that:

- all Personal Data must be processed lawfully, fairly and transparently;
- Personal Data shall be obtained only for one or more specified and explicit lawful purpose(s) (purpose limitation);
- Personal Data shall be adequate, relevant and necessary (data minimisation);
- 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) (storage limitation);

- Personal Data shall be processed in accordance with the rights of data subjects under the data protection legislation;

- 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 using appropriate technical or organisational measures (integrity and confidentiality); and

- Personal Data shall not be transferred to a country outside the European Economic Area unless an adequate level of protection is in place (See section 15).

4.3 The Data Protection Officer is responsible for advising staff at the University of their obligations pursuant to data protection legislation and for monitoring compliance with the legislation.. 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 Protection Officer and Data Control Officer(s) are recorded in Appendix One.

4.4 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, or appoint a new service provider, or procure a new IT system or technology, 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 data protection legislation and, if it does, so they may update the Notification in advance of such change or otherwise as soon as possible. Do not start to collect new Personal Data, or use Personal Data for new purposes, or appoint new service providers to use Personal Data, or contract for new IT systems or technology which stores or uses Personal Data without their prior written approval.

4.5 All those to whom the Policy applies should not use University facilities to Process Personal Data for purposes unconnected with their employment, engagement or their studies (if they are a student of the University) or for domestic or personal purposes. Such processing is not covered by the University Notification and in such cases each employee will be individually responsible for compliance with the obligations under the data protection legislation.

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

- the ICO relating to the University's data Processing activities;

- any individual looking to exercise his/her rights under the data protection legislation;

- 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.

5. What does "fair, lawful and transparent use of Personal Data" mean?

5.1 One of the main data protection obligations requires the University to process Personal Data fairly, lawfully and transparently. In practice, this means that the University (and each staff member, student consultant, contractor, agent and service provider) must comply with at least one of the following conditions when processing Personal Data:

- the individual to whom the Personal Data relates has consented to the processing;
- the processing is necessary for the performance of a contract between the University and the individual or another person;
- the processing is necessary in order to protect the vital interests of the individual;
- the processing is necessary to comply with a legal obligation placed on the University; or
- the processing is necessary in order to pursue the legitimate interest of the Data Controller (i.e. the University) and is not unfair to the individual.

5.2 Reliance on these conditions must be discussed with the Data Control Officer(s) prior to being relied upon. All new data processing activities and projects involving the use of Personal Data must be notified to the Data Protection Officer prior to being started.

6. What is a privacy notice?

6.1 When an individual gives the University any Personal Data about him or herself, the University must make sure the individual knows:

- that the University is the Data Controller and is responsible for the processing of their Personal Data;
- for what purposes that entity will process the Personal Data provided to it for;
- has sufficient information on any disclosures/transfers of that information to third parties; and
- Any other information that the individual should receive to ensure the processing carried out is within his/her reasonable expectations.

6.2 Providing this information is known as providing a "privacy notice". The University should give individuals appropriate Privacy Notices when collecting Personal Data about them.

6.3 You should only process Personal Data in a manner and for purposes consistent with the relevant privacy notice(s) provided to each relevant individual.

6.4 Even with consent or if one of the other lawful reasons for processing applies, the University cannot make any use it wants of Personal Data. All the other rules

explained in this Policy still have to be complied with. For example, the University still has to satisfy the other requirements described below in this Policy, such as making sure the information collected is not excessive. Simply because a person has consented to giving you their information does not override that restriction. Similarly, Personal Data must not be used in a way which would infringe another law, for example, for bribery, or racial, age, sexual, or disability discriminatory purposes. To do so would render its collection and use also unlawful.

6.5 Where collecting Personal Data about an individual indirectly (e.g. from a published source), you must ensure there is suitable evidence that the provider has the lawful right to disclose these details to the University for the envisaged use by the University. If in doubt, the University must inform the individual that it holds the data and the purposes for which that data will be used.

6.6 If the information is not received directly from the individual concerned, then the University must ensure that the individual is given all the relevant information in the privacy notice as soon as possible, at the latest within a month (and before any disclosure or transfer of their details) and that the University has authority to use this information.

6.7 You must not buy in any Personal Data about individuals, or carry out any activities involving any data enhancement or enrichment or matching, without prior written approval from the Data Protection Officer.

6.8 Under GDPR, there are strict requirements about information which must be provided to individuals in privacy notices. You must ensure that you only use the appropriate University approved privacy notices. Such privacy notices must include:

6.8.1 contact details of the Data Protection Officer;

6.8.2 legal basis for processing;

6.8.3 if legal basis is “legitimate interests”, state those interests;

6.8.4 categories of recipient(s) of personal data;

6.8.5 details of any transfers of data outside the EEA and the safeguards in place to protect data;

6.8.6 period of retention/criteria applied;

6.8.7 individual’s rights in relation to their data;

6.8.8 the right to withdraw consent (if consent is relied upon);

6.8.9 the right to lodge a complaint with the ICO; and

6.8.10 whether any automated decision making takes place and consequences of processing.

7. Data Collection

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

- the nature of information being collated or held to ensure there is a sound business reason for doing so;
- the length of time Personal Data is being held and whether this complies with the University's legal obligations;
- 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 data protection legislation.

7.2 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 data protection legislation.

7.3 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.

7.4 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. This includes anonymisation of Personal Data and use for research analysis.

8. What is Sensitive or Special Categories of Personal Data and what conditions need to be met when dealing with it?

8.1 "Sensitive or Special Personal Data" is Personal Data about a person's race or ethnicity, their health, their sexual preference, their religious or philosophical beliefs, their political views, trade union membership or information accusing an individual of any crime, or about any criminal prosecution against them, and the decision of the court and any punishment. Under GDPR, Special Categories of Personal Data also includes biometric data for unique identification and genetic personal data.

8.2 The Data Control Officers can provide you with further information on what is Sensitive Personal Data and you should comply with their advice in respect of that data.

8.3 Where collected, Sensitive or Special Categories of Personal Data should not be used unless strictly necessary. Extra care must be taken with it (in addition to the normal rules for Personal Data) and it must be kept more securely. There are special obligations under the data protection legislation with which the University must comply when processing Special Categories of Personal Data to limit its collection and use and to ensure it is treated more securely than other details. Additional restrictions are placed on top of the lawful reasons for processing Personal Data mentioned above. For example, it is difficult to lawfully use such details without the consent of the individual, which has to be explicit, free,

voluntary, in writing and obtained prior to processing any Sensitive or Special Categories of Personal Data.

8.4 The University does not generally seek to obtain Sensitive or Special Categories of Personal Data unless:

- the individual concerned agrees in writing that we may do so, on the basis of a full understanding of why the University is collecting the data;
- the University needs to do so to meet its obligations or exercise its rights under employment law; or
- in exceptional circumstances such as where the processing is necessary to protect the vital interests of the individual concerned (i.e. in "life or death" circumstances).

8.5 Employees should note that the "legitimate interest" criteria described above (in clause 5.1) alone is not enough to process Sensitive or Special Categories of Personal Data.

8.6 Sensitive or Special Categories of Personal Data should not be emailed or disclosed unless measures are taken to encrypt or otherwise secure that information due to the potential for harm or distress if the email is received by unintended recipients or otherwise goes astray. Sensitive or Special Categories of Personal Data should be collected and used as little as possible, be subject to more limited and strictly need to know access and used subject to greater security measures than other details.

9. Disclosure of Data

9.1 To ensure compliance with the data protection legislation 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:

9.1.1 Save for statutory compliance or as permitted by the data protection legislation, it must only be used for one or more of the purposes specified and notified to or reasonably expected by the relevant individuals.

9.1.2 Provided that the identification of individual employees/students is not disclosed, aggregate or statistical information may be used in accordance with the ICO's Code on Anonymisation to respond to any legitimate internal or external requests for Personal Data, e.g. OfS 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. The HESA collection notices which provide information to students and staff about what happens to their data when it is sent to HESA can be found here: https://www.hesa.ac.uk/collection-notices.

9.1.3 Personal Data must not be disclosed, either within or outside the University, to any recipient who is not authorised to receive it, in any circumstances contrary to the obligations placed on the University

under the data protection legislation (and in this Policy), 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 as set out in this Policy. Disclosures to outside the University can only be made if permitted by the data protection legislation, 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).

9.1.4 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).

Requests for Personal Data

9.2 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 data protection legislation, as well as being proportionate to need.

9.3 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 can be made orally or in writing and members of staff should be satisfied about the legitimacy of requests for information and seek valid documentary evidence where appropriate. In the case of a request by an individual for the own Personal Data, also known as a Subject Access Request (SAR), the information should be provided free of charge. A reasonable administrative may be charged in certain circumstances but advice should be sought from the Data Protection Officer before any charge is made.

9.4 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:

9.4.1 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.

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

9.4.3 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.

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

9.5 Examples of requests for Personal Data by third parties, which do require the consent of the data subject are:

9.5.1 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.

9.5.2 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 below in section 13.

9.6 See also section 12.8 on individual subject access requests for how the University deals with such disclosures.

10. Third party contractors

10.1 The University may use Third Parties to provide services to it - for example, running its IT systems or to run a marketing campaign. Where such Third Parties use the University's Personal Data, special rules apply. The University must have in place a written contract with that Third Party which contains specific limitations on what they can do with the Personal Data and places security obligations upon them. Please contact your Data Protection Officer who will be able to provide you with the appropriate wording to include. You must not contract with such a Third Party without this wording being included. The University is responsible for their use of its Personal Data and so this is important.

11. Data should be necessary and accurate

11.1 The Personal Data you collect should be appropriate to and sufficient for the relevant purpose(s) you are collecting it for, but not excessive for that purpose(s). Only process the Personal Data which is necessary for the task; minimise your use of Personal Data rather than maximise it. Don't collect and process more Personal

Data than you really need. In the end, it simply adds to the University's compliance burden and storage costs. For example, if you will never telephone someone at home, you do not need their home telephone number.

11.2 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.

11.3 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.

11.4 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 e.g. it could lead to an inaccurate record of events. In such cases, please liaise with Data Protection Officer for assistance (please see below).

12. Individuals' Rights

12.1 Individuals have rights in relation to information processed about them. Under GDPR these rights change and expand and in some cases will depend on the basis on which Personal Data is used eg by consent, or to perform a contract, or where required by law. Certain rights in relation to their Personal Data are:

12.1.1 the right to access, rectification, erasure, restriction or to object to Personal Data held about themselves;

12.1.2 the right to prevent Processing of Personal Data for direct marketing purposes and in certain circumstances, the right to withdraw consent to processing at any time;

12.1.3 the right to know the period for how long the data will be stored and a right to data portability ;

12.1.4 the right to be informed of automated decision making; and

12.1.5 the right to lodge a complaint with the Information Commissioner.

12.2 Individuals 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 12.9 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).

12.3 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. 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.

12.4 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.

12.5 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.

12.6 Assessment results must not be given over the phone.

12.7 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.

12.8 The recipient of a subject access request must immediately refer it to the relevant Data Control Officer. The request may be in writing or submitted orally and the Data Control Officer must respond promptly on behalf of the University within one month from the date on which the request was first received (subject to paragraph 12.7). Further guidance is available on docshare on how to deal with a SAR. 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.

12.9 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:

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

12.9.2 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;

12.9.3 Personal Data which consists of records of the intentions of the University relating to any negotiations with the individual to the extent that disclosure would be likely to prejudice those negotiations only;

12.9.4 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.

12.10 In addition to seeking disclosure of information, an employee/student or other individual 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/student 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.

12.11 The individual 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 individual or it is necessary for the performance of a contract to which the individual is a party.

12.12 An employee/student or other individual 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.

12.13 In the event of a complaint in relation to this Policy, students should use the official Complaints Procedure published on the University website, whilst employees should use the Grievance Procedure.

12.14 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 registration with the Information Commissioner as a Data Controller in its own right. The Data Controller will liaise with a member of the Student Union to try to ensure that Personal Data is properly notified.

13. Security and Security Breach Management

13.1 This Policy should be read with the Information Security Policy and Records Management Policy.

13.2 In order to prevent accidental or unlawful destruction, loss, alternation, unauthorised disclosure of or access to Personal Data transmitted, stored or otherwise processed, the following security measures will be required in respect of the processing of any Personal Data:

13.2.1 Access to Personal Data on staff and students is restricted to those members of staff who have a legitimate need to access such data..

13.2.2 Members of staff authorised to access Personal Data under paragraph 13.2.1 above, will be allowed to do so, only in so far as they have a legitimate need to do so and in accordance with the University's fair processing notice.

13.2.3 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 trained in their use.

13.2.4 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 may result in a formal disciplinary investigation.

13.2.5 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 may lead to a formal disciplinary investigation.

13.2.6 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 or Special Categories of 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. If it is necessary to transfer large volumes of personal data, do so using an IT approved transfer facility.

13.2.7 Extra care is needed to secure Sensitive or Special Categories of Personal Data because more damage is likely if it is lost. For example, if details of an individual's medical condition got into the wrong hands it would be very distressing for that individual. Be especially careful if you want to send Sensitive or Special Categories of Personal Data to another person - whether that is by fax or email - that it is sufficiently secure and can only be received and accessed by the intended recipient. A password protected attachment is not enough.

13.2.8 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.

13.2.9 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.

13.3 The University also recognises that adequate security is important where it arranges for outside service providers to process Personal Data on its behalf. Where such arrangements are established by the University, service providers must be bound by written contracts to protect the Personal Data provided to them.

13.4 Under GDPR, the University must record all security breaches affecting it and its Personal Data. In many cases, the University will be obliged by law to inform the Information Commissioner of such breaches within 72 hours and may also need to inform affected individuals.

13.5 Accordingly, if you become aware of any security beach (including any accidental or unlawful destruction, loss, alternation, unauthorised disclosure of or access to Personal Data transmitted, stored or otherwise processed by the University) you must immediately inform the Data Protection Officer. Please note that failure to report security breaches promptly (within 48 hours) may amount to a disciplinary offence as it could put the University in breach of its legal obligations.

14. Third Parties

14.1 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 data protection legislation and this Policy.

15. Transfer of Data outside the European Economic Area

15.1 It is a requirement of the data protection legislation 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 server in Europe, being remotely accessed from abroad.

15.2 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. The countries currently deemed adequate include the USA (to the extent the recipient company has a suitable and Privacy Shield certification), Andorra, Argentina, the Faroe Islands, Guernsey, Jersey, Isle of Man, Switzerland, and Canada (commercial organisations), Israel, Uruguay and New Zealand.

15.3 The University may also transfer Personal Data outside the EEA to a recipient:

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

15.3.2 who has other arrangements which provide adequate safeguard for the Personal Data, as recognised by the ICO. Please liaise with Data Protection Officer for any queries about such arrangements.

15.4 There are specific and very limited 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 only with the prior consent of Data Protection Officer. The University must keep records of all such transfers and why they are adequately safeguarded.

16. Student use of Personal Data

16.1 Where students process Personal Data for the purposes of research or study or in pursuit of an academic qualification, they should inform their supervisor or unit leader. Members of staff directly supervising or teaching such students should ensure that the Personal Data being processed is adequately covered by the University's fair processing notice. Guidance may be sought from the Data Protection Officer. Awareness of the need to comply with this Policy should be promoted to students through publications such as the 'Dissertation Guidelines'.

16.2 If Personal Data processed by students is not covered by the University's fair processing notice, staff must make students aware that such processing will be deemed to be for the students' own personal or domestic purposes. Staff shall make such students aware of what students need to do to comply with the Data Protection Act and of the appropriate level of security arrangements which attach to the particular set of Personal Data.

17. Contractors and Suppliers

17.1 In certain circumstances, it may be necessary to allow contractors or suppliers access to Personal Data in the course of maintenance or repair work.

17.2 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.

17.3 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:

17.3.1 the University must enter into a written contract with the Data Processor to confirm the third party's appointment as Data Processor;

17.3.2 the contract must state that the Data Processor will only use the Personal Data in accordance with the University's instructions; and

17.3.3 the contract must state that the Data Processor is to keep the Personal Data secure in accordance with its obligations under the data protection legislation.

18. Appropriate due diligence is required in advance on such providers to ensure they are suitably secure and reliable. Suitable due diligence checklists and contract wording is available from the Data Protection Officer. You must not use or agree to other forms of wording without prior written approval from the Data Protection Officer.

18.1 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 data protection legislation and that any necessary contractual terms are in place.

19. Staff use of Personal Data off-site, on mobile devices, home computers or at remote sites

19.1 Employees, consultants, agents and service providers processing Personal Data off-site and on mobile devices 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. Staff issued with mobile devices by the University must register such devices with IT to ensure that appropriate security controls and settings have been applied.

19.2 You should at all times:

19.2.1 attempt to minimise the amount of Personal Data that is processed off-site and only do so where absolutely necessary;

19.2.2 keep a record of all Personal Data taken off-site and when it was returned;

19.2.3 never leave the Personal Data unsupervised or unsecured;

19.2.4 ensure you 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; and

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

20. Use of Personal Data in Research

20.1 The data protection legislation provides certain exemptions for 'research purposes' including statistical or historical purposes.

20.2 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:

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

20.2.2 held indefinitely;

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

20.3 The Data Protection Principles 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.

21. Collection of Personal Data from University Web Pages

21.1 The University will provide the following information on any University Web pages designed to collect Personal Data:

21.1.1 The identity of the University as the responsible data controller under the data protection legislation;

21.1.2 the purpose(s) for which the Personal Data is being collected;

21.1.3 the recipients or classes of recipients to whom the Personal Data may be disclosed;

21.1.4 an indication of the period for which the Personal Data will be kept;

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

21.2 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.

21.3 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 Communications (EC Directive) Regulations 2003 as amended or replaced by subsequent legislation. Please liaise with the Data Protection Officer for more details.

22. Marketing

22.1 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 relevant data protection and ePrivacy legislation.

22.2 As with other types of processing, the use of Personal Data for marketing purposes must satisfy the fair and lawful use requirements set out above. This means information notices must be given, and a lawful reason for processing has to be satisfied. Typically, this will have to be consent. You therefore should not use Personal Data to contact individuals for marketing purposes (including sole traders and individual members of business partnerships) by email, text or similar unless the individual has consented to marketing use.

22.3 Individuals have a right to decline postal marketing. Where marketing is to be by email, text or similar electronic means, their consent is needed and must clearly cover marketing by email, text or similar. Special rules apply to when consent is needed and how consent is obtained (for example, whether individuals can "opt out" of or "opt in" to receiving marketing) depending on the type of marketing contemplated and the means of communication with the individual. Special rules apply to facilitate prompt action regarding objections to marketing.

22.4 It is advisable to check the scope of any marketing consent you are relying upon, particularly if you are sending information relating to other group companies, Third Parties or contemplating sharing the Personal Data with a Third Party to allow them to do so. If you are obtaining Personal Data from a Third Party for marketing use, then you should check that the consents they have obtained permit disclosure to the University and the intended processing by the University. Consent must be the appropriate form of consent.

22.5 You must promptly comply with any request by an individual not to receive direct marketing (where it is addressed to them) or their choice not to receive marketing by a particular method (for example, post, fax, telephone, email or text messaging).

APPENDIX ONE

UNIVERSITY OFFICERS

Data Protection Officer	Sarah Martin, University Solicitor Email: dpo@uca.ac.uk
Responsibility:	Data Protection Policy Annual Registration Advising on policies relating to third party data
Data Control Officers	Angela Fisher, Director of Human Resources
Responsibility:	Advising on policies relating to staff data
	Andrew Penman, Registrar
Responsibility:	Advising on policies relating to student data