Data Protection Policy Revised 2020

1 Introduction

1.1 The University holds and processes information about employees, students and other data subjects for academic, administrative and commercial purposes. When handling such information the University and all staff or others who process or use any personal information must comply with the Data Protection Principles, which are set out in the General Data Protection Regulations (GDPR).

1.2 These principles state that personal data shall:

1.2.1 be processed lawfully, fairly and in a transparent manner in relation to individuals;

1.2.2 be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

1.2.3 be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

1.2.4 be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

1.2.5 be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

1.2.6 be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

2 Definitions

2.1 "Personal Data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or

more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

2.2 "Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

2.3 "Processor" means a natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller;

2.4 "Consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

2.5 "Data Protection Officer" (DPO) is the designated person with responsibility for training staff and ensuring compliance on a day-to-day basis.

2.6 "Staff", "student" and "other data subjects" may include past present and potential members of these groups.

2.7 "Other data subjects" and "third parties" may include contractors, suppliers, contacts, referees, friends or family members.

2.8 "Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

2.9 All references to GDPR throughout this document also include any secondary legislation and prior legislation that has not been repealed.

3 Status of the policy

3.1 This policy does not form part of the formal contract of employment but it is a condition of employment that employees will abide by AUB policies. Failure to follow the policy can therefore result in disciplinary proceedings.

3.2 Any member of staff who considers that the policy has not been followed in respect of personal data about him or herself should raise the matter with the Data Protection Officer who will offer advice and/or seek to resolve the matter as an informal complaint. The full complaints procedure is detailed at section 10.

3.3 Managers are responsible for ensuring that their staff adhere to the Data Protection Policy and should: set an example of good practice themselves; challenge poor practice and encourage and promote good practice among their teams.

4 Notification of data held and processed

4.1 All staff, students and other users are entitled to:

- know what information the University holds and processes about them and why
- know how to gain access to it
- know how to keep it up to date
- know what the University is doing to comply with its obligations under the GDPR

4.2 Information provided confidentially, whether explicitly or implicitly, will not normally be disclosed. Exceptions will be made only on the grounds of public interest; when disclosure is required by law; or where consent is given. In such cases, the source of the information will normally be informed of the intention to disclose.

4.3 There may be occasions when the legislation appears to be in conflict such as when one person seeks information which was given in confidence by another person. In this situation the University will seek to meet the request by redacting information, providing confidentiality can be maintained where appropriate.

4.4 The Data Protection Officer will review the use of personal data on an annual basis, to ensure that the list of uses is both comprehensive and up to date. Any changes will be noted in the policy, and will be notified to all data subjects who are affected.

4.5 Individuals will normally be asked for their permission before data is passed to third parties. If permission is not required, for example if the University has a statutory requirement to provide the information, individuals will be notified of this decision and the action that will be taken.

5 Responsibilities of staff

5.1 All staff are responsible for checking that information that they provide to the University in connection with their employment is accurate and up to date and informing the University of changes to or errors in information held.

5.2 As part of their responsibilities, staff may collect information about other people (e.g., about students' course work, opinions about ability, references to other academic institutions, details of personal circumstances). They must follow the guidance laid out in this policy.

5.3 Staff providing references for students should consult the document Guidance on writing references for students, which is on the intranet.

5.4 Staff should note that all students are treated the same under the GDPR so if parents / guardians or any other person contacts the University wishing to discuss a student that student must give written permission before any discussions can take place.

5.5 If staff remain unsure of their obligations as data processors they should seek guidance from the Joint Information Systems Committee (JISC) Code of Practice for the HE sector and the Data Protection Officer.

5.6 It is the responsibility of any member of staff who takes personal data off campus to ensure that it is held securely, encrypted or password protected.

5.7 If staff borrow equipment such as a laptop or any other device for use off campus they are held responsible for ensuring any personal data are removed before it is returned in line with the Staff Laptop Policy.

5.8 If a member of staff receives a request for information about a third person from the Police they should pass the request to the Data Protection Officer. S/he should not attempt to deal with it themselves.

6 Responsibilities of students

6.1 Students must ensure that all personal data provided to the University are accurate and up to date. Students can update their own contact details through e-vision: staff should tell them how to do this rather than taking the details and passing them on.

6.2 As part of their studies, students may from time to time process personal data, for example, in conducting questionnaires or carrying out other quantitative research and if this is the case, they should read the Research Ethics Policy. If they intend to use University computer facilities for this processing, they must notify the Data Protection Officer.

6.3 If students borrow equipment such as a laptop for use off campus they are held responsible for ensuring any personal data are encrypted or password protected and that the data are removed before it is returned, in line with the Student Laptop Policy.

6.4 Any student who considers that the policy has not been followed in respect of personal data about him or herself should raise the matter with the Data Protection Officer initially. If the matter is not resolved, it should be dealt with under the Complaints Procedure, which is detailed in section 10.

6.5 All students are treated the same under the GDPR so if parents / guardians or any other person contacts the University wishing to discuss a student that student must give written permission before any discussions can take place.

6.6 To give written permission students need to complete the third party consent form, which they can do via MyAUB and eVision. On the form, they can choose the types of information that can be shared and with whom. They should update the information when necessary and they can change their minds about giving permission at any time by going back to the form, deleting the names and unchecking the boxes.

7 Data Subject Rights

7.1 The GDPR sets out specific rights for all individuals whose data is subject to processing:

7.1.1 The right to be informed: transparency is a key requirement of the GDPR. The University is required to provide clear and concise information about how personal data will be processed.

7.1.2 The right of access: this gives individuals the right to obtain a copy of their personal data and supplementary information. The right of access is explained in more detail in section 8.1.

7.1.3 The right to rectification: this gives individuals a right to have inaccurate personal data rectified.

7.1.4 The right to erasure: this right is not absolute and will only apply in specific circumstances. Individuals can ask to have personal data erased.

7.1.5 The right to restrict processing: this right is not absolute and will only apply in specific circumstances. Individuals have the right to request the restriction or suppression of their personal data.

7.1.6 The right to data portability: this allows individuals to obtain and reuse personal data for different services.

7.1.7 The right to object: individuals have a right to object to data being processed in certain circumstances. If applicable, this right allows individuals to stop personal data from being processed.

7.1.8 Rights related to automated decision making including profiling: this applies to all automated individual decision-making and profiling.

8 Rights to Access Information

8.1 Students are entitled to information about their marks for assessed work. The University will normally withhold certificates, accreditation or references in the event that any debts owed to the University have not been paid or any University property returned.

8.2 Staff, students and others have the right to access any personal data that the University keeps about them, either on a computer or in paper files, subject to the factors mentioned at 4.3.

8.3 Any person who wishes to exercise this right should complete the University Subject Access Request form obtainable from HR or the Data Protection Officer.

8.4 A reasonable fee for access to this data will only be charged if a request is manifestly unfounded or excessive, particularly if it is repetitive or is a request for duplicate copies of information.

8.5 Under the GDPR, requests must be responded to without delay and at the latest within one month of the request. This period can be extended by a further two months where requests are complex or numerous. The University will comply with requests for access to personal information as quickly as possible.

8.6 Information requested will be supplied in a format appropriate to the needs of the enquirer, where reasonable.

9 Children's Data

9.1 The University acknowledges its responsibilities when processing children's data and considers anyone under the age of 18 a child.

9.2 When consent is used as the legal basis for processing personal data, care will be taken to ensure such consent is sought from a parent or guardian.

9.3 The University has a Safeguarding Policy to ensure children are protected; the principles of both this Data Protection Policy and the Safeguarding Policy must be considered when processing children's data.

10 Data Security

10.1 Unauthorised disclosure of personal data could result in action being taken against the University under criminal law.

10.2 All staff and students are responsible for ensuring that:

- Personal data they hold, in whatever format, are kept securely and for no longer than necessary, in line with University retention schedules.
- Personal information is not disclosed either orally or in writing, accidentally or otherwise, to any unauthorised third party.

10.3 The security of digital personal information is covered in the Computer and Data Security Policy.

10.4 Personal information held in a paper format should be kept under lock and key. If it is computerized information, and kept where it may be seen by unauthorised staff or students, it should be encrypted or password protected; or kept only on disks which are kept securely.

10.5 At the end of the retention period data will be disposed of securely.

10.6 Unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

10.7 Personal data will not be sent to companies or countries outside the European

Economic Area (EEA) without confirmation that the data is treated in line with the GDPR.

10.8 Where data are sent to external organisations within the EEA, (for example staff payroll), this will be notified to the data subject in advance and the University will require sight of the company's Data Security Policy before passing them the data.

10.9 All personal data held by the University, irrespective of its source, will be handled in accordance with the GDPR.

11 Publication of Information

11.1 It is University policy to make as much information public as possible, within the requirements of the GDPR and Freedom of Information Acts. The University maintains a publication scheme approved by the Data Protection Officer.

11.2 The University has notified the Data Protection Officer that personal information may need to be processed for the following purposes:

1. Staff Administration
2. Advertising, Marketing, Public Relations
3. Accounts & Records
4. Property management
5. Education
6. Crime Prevention and Prosecution of Offenders

11.3 The Information Commissioner's Office has a section on his website on GDPR, which explains the Act and how individuals can use it.

12 Complaints procedure

12.1 The University takes its obligations under the GDPR very seriously. If, for any reason, you are dissatisfied with the way in which the Policy has been implemented, a Subject Access Request has been handled or how your data has been processed, you may invoke the following complaints procedure.

12.2 The Complaints Procedure is split into informal and formal complaints. The University hopes to be able to resolve most complaints on an informal basis. You are asked to pursue the informal complaints procedure before invoking the formal complaints procedure.

12.3 Informal Complaints Procedure

12.3.1 Contact the Data Protection Officer in writing at Arts University Bournemouth, Wallisdown, Poole BH12 5HH or by email (dp@aub.ac.uk) and she will try to resolve the complaint informally.

12.3.2 The Data Protection Officer must respond to your complaint within 20 working days.

12.3.3 If you are dissatisfied with the outcome, or do not receive a response within 20 working days, you are entitled to invoke the formal complaints procedure (see below).

12.4 Formal Complaints Procedure

12.4.1 If you are dissatisfied with the outcome of an informal complaint, you must make a formal complaint in writing, and provide supporting evidence/paperwork;

12.4.2 Address your written complaint to the University Secretary and Registrar, Arts University Bournemouth, Wallisdown, Poole BH12 5HH. If the complaint concerns the University Secretary and Registrar another member of the University Management Team will deal with the formal complaint.

12.4.3 The University Secretary and Registrar (or alternate) will investigate and respond to your complaint within 20 working days.

12.4.4 If you are dissatisfied with the outcome of the University's formal complaints procedure you may refer the matter to the Information Commissioner.
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

The Arts University Bournemouth is committed to the provision of a working and learning environment founded on dignity, respect and equity where unfair discrimination of any kind is treated with the utmost seriousness. It has developed and implemented an Equality and Diversity Plan to guide its work in this area. All the University's policies and practices are designed to meet the principles of dignity, respect and fairness, and take account of the commitments set out in the Equality and Diversity Plan. This policy has been subject to an equality analysis to ensure consideration with regard to the provisions of the Equality Act 2010.

Date of last EA review: 01/2018

Related documents

Process for Data Protection
Data Protection Guidelines
Safeguarding Policy
Computer and Data Security Policy
Freedom of Information Publication Scheme
Guidance on writing references for students
Research Ethics Policy
Staff Laptop Policy
Student Laptop Policy
Subject Access Request form