DATA PROTECTION POLICY

1. INTRODUCTION

1.1 This policy document supports the University's Information Governance Framework and to ensure compliance with data protection law and regulation.

1.2 All personal data must be processed in accordance with this policy and the Data Protection Act 2018 ('DPA') and the General Data Protection Regulations 2016 ('GDPR') or any successor legislation to the GDPR or the DPA. Failure to comply may result in disciplinary action or even criminal proceedings.

2. SCOPE

2.1 The policy covers all processing of personal information by the University.

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

3. GOVERNANCE (Responsibility and Accountability)

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

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

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

3.1.3 Deans of Schools and Directors of service are responsible for ensuring that:

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

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

(c) the processing of personal data is audited periodically, and any subsequent action plans followed through appropriately.

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

4. INFORMATION ASSET REGISTERS

4.1 All Schools and service areas must create and maintain a complete register of their manual and electronic systems that contain personal data. This record of processing activities should also identify the legal basis for processing the personal data.

5. ANNUAL AUDIT OF PERSONAL DATA PROTECTION

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

5.1.1 raise general awareness of data protection;

5.1.2 demonstrate the University's commitment to data protection;

5.1.3 confirm that adequate controls exist;

5.1.4 identify any potential breaches of compliance;

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

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

6. DATA PROTECTION IMPACT ASSESSMENTS

6.1 Where appropriate, for example where new systems or major changes are contemplated to systems or processes involving personal information, Data Protection Impact Assessments (DPIAs) must be used to identify potential issues and risks. Guidance regarding when and how to conduct a DPIA is available on the University's Data Protection page and from ICO DPIA guidance. Advice is also available from the Information Compliance Team at: infocompliance@leedsbeckett.ac.uk.

7. TRAINING

7.1 All staff and volunteers need to understand the importance of personal information processing and storage. Every member of staff will complete an online data protection training module. This will be refreshed every three years and supplemented by face-to-face training for identified staff. Responsibilities will also be explained to new members of staff during induction and appropriate additional training will be provided for employees who have responsibility for processing and/or management of personal data and/or information.

8. PRINCIPLES FOR PROCESSING PERSONAL DATA

8.1 The University must comply with DPA's principles and has overall responsibility for accountability under data protection law. This also means that we must ensure that personal information:

8.1.1 is obtained lawfully, fairly and in a transparent manner;

8.1.2 is used only for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

8.1.3 is adequate, relevant and limited to the purpose;

8.1.4 is accurate and kept up to date;

8.1.5 is not kept for longer than is necessary for the purpose;

8.1.7 is protected from unauthorised access, accidental loss or destruction;

8.2 The University must also maintain records to show how we comply with the principles when processing personal data and how we meet our legal obligations to comply with DPA.

8.3 In addition to the principles outlined above, the University must also ensure that personal data is processed in accordance with individuals' rights. These are the right to:

- access their personal data
- be informed about uses of their personal data
- rectification
- erasure ("right to be forgotten")
- restriction of processing
- portability
- object to automated decision making
- object to processing on the basis of legitimate interest or the public task of the data controller
- object to processing for purposes of direct marketing

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

9. DEFINITIONS WITHIN DPA

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

9.1.1 DPA covers *all* personal data processed by the University, irrespective of whether these are held by individual members of staff in their own

separate files (including those held outside the University campuses) or in departmental records systems or central systems of the University.

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

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

9.1.4 Personal Data includes name, address, telephone number, email address, location data and IP address.

9.1.5 Special Category Personal Data includes information relating to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, biometric data and genetic data. Under DPA the processing of special category data is subject to much stricter conditions. In particular, processing of special category data requires explicit consent. However, in most instances consent to process special category data is obtained routinely by the University.

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

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

10. ELECTRONIC DATA SYSTEMS

10.1 Electronically held data encompasses not just the use of personal data held on databases but, for example, emails, letters and other documents held on disk, hard drive, mobile devices and in cloud based servers.

11. MANUAL FILING SYSTEMS

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

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

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

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

12. THE LAWFUL BASIS FOR PROCESSING PERSONAL DATA

12.1 To process personal data lawfully, we must have a legal basis under Article 6 for the processing. This means that at least one of the following must apply:

- We have the consent of the data subject to the processing;
- the processing is necessary to fulfil a contract, or in preparation for a contract, with the data subject;
- the processing is in the vital interests of the data subject;
- we have a legal obligation to process the personal data;
- we have a public function that requires the processing;
- it is in our legitimate interests to process the personal data considering the data subjects' legitimate interests.

12.2 To process special category data, we must have both a lawful basis under Article 6 above and a separate condition for processing under Article 9. This means that one of the following must also apply: The University has a duty, under certain circumstances, to ensure that members of staff are suitable for the job, and students for the courses offered. On occasion, checks with the police or Disclosure & Barring Service will be required to verify criminal records. (There are, for example, some jobs or courses that will bring the applicants into contact with children and/or vulnerable adults.) Where this is relevant to the job, the University may also ask for information about particular health circumstances. In such circumstances, the University will normally at the time of application advise applicants that they intend to seek such information and/or seek self-disclosure.

12.3 In most instances staff, (and where appropriate, students), will not need to obtain consent to process from data subjects either because one of the other legal basis apply or because, where consent is required, it is obtained routinely by the University. Upon registration, students are notified via the Student Privacy Notice of the ways in which their personal data will be used. Likewise, the Colleague Privacy Notice sets out how the University will use employees' personal data on acceptance of an offer of employment.

13. ACCESS TO DATA

13.1 Staff, students and others in contact with the University have a general right of access to personal data that is being kept about them either on computer or in 'relevant' manual files. Any person who wishes to exercise this right should contact Governance and Legal Services: infocompliance@leedsbeckett.ac.uk. Data Subject Access Request forms are available from this office and on the website. There is no entitlement to immediate or on-site access to information. HE Institutions have a maximum of one calendar month in which to comply with a request for access by a data subject.

13.2 All enquiries from the police or other statutory agencies requesting access to data about individuals must be referred without delay to the Head of Information Governance, Governance and Legal Services.

14. STAFF OBLIGATIONS

14.1 Many staff members have responsibilities for processing personal data about students (and in some instances, colleagues) as well as being data subjects in their own right. In connection with personal data about students and colleagues, all staff must comply with University guidelines on data protection. Colleague, potential colleague and student privacy notices are available as separate documents.

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

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

14.2.2 inform the University of any changes for which they are responsible, for example change of address.

15. STUDENT OBLIGATIONS

15.1 Students are advised at registration and enrolment about the information the University will collect, use and retain about them, and those to whom such information will be disclosed. Students must ensure that all personal data provided to the University are accurate and up to date. They must ensure that any changes, of address, for example, are notified to Registry Services, to their School and to other offices as appropriate and without delay, in accordance with the Student Contract.

15.2 Students may come into contact with personal data through the University for the purposes of research or study, in pursuit of an academic qualification and under the direct supervision of a member of staff. In such cases, staff must notify students about, and students must abide by, the relevant provisions of this guidance.

16. DATA SECURITY

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

16.1.1 any personal data which they hold are kept securely;

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

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

16.3 Managers must ensure that, where a data processor processes data on the University's behalf (a mailing agency, for example), there is a written contract between the parties. The contract should specify that the processor agrees to act on the University's instructions and to abide by the provisions of the law. Advice on data sharing is available from Information Compliance Team: infocompliance@leedsbeckett.ac.uk.

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

16.4.1 kept in a lockable room with controlled access; or

16.4.2 kept in a locked filing cabinet; or

16.4.3 in a locked drawer; or

16.4.4 if computerised, be password protected; or

16.4.5 kept only on disks that are themselves kept securely.

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

16.6 Off-site use of personal data presents a potentially greater risk of loss, theft or damage to personal data; and the institutional and personal liability that may accrue from the off-site use of personal data is similarly increased. Staff and students should take particular care when laptop computers or personal machines are used to process personal data at home or in other locations outside the University. Staff and students should also be aware that this policy and their responsibilities under it apply when data are processed under such circumstances. Additional guidance is available in the suite of Information Management and Security policies.

17. DISPOSAL AND DESTRUCTION OF PERSONAL DATA

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

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

18. SHORT-TERM AND VOLUNTARY STAFF

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

19. VENDORS, CONTRACTORS, AND SUPPLIERS

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

20. PUBLICATION OF UNIVERSITY INFORMATION

20.1 It is the University's policy to operate with openness and transparency; in particular the following information may be available publicly (including on the University website):

20.1.1 lists of staff;

20.1.2 names and work contact information of staff;

20.1.3 University e-mail addresses;

20.1.4 photographs of staff and academic profiles;

20.2 It is recognised that there might be occasions when a member of staff or student has good reason for wishing details in certain of these lists or categories to remain confidential or to be restricted to internal access. In such cases, they should contact the Information Compliance Team for advice. In connection with the publication of photographic images of staff, particularly on web pages, all members of staff are advised that such images should not be made publicly accessible without the consent of the individuals concerned.

21. MONITORING OF COMMUNICATIONS AND USE OF CCTV

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

21.2 In all instances:

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

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

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

21.3 Students or staff members who consider that the positioning of a close circuit television camera or use of a webcam is inappropriate should contact the Information Compliance Team.

22. INTERNET AND EMAIL USE

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

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

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

23. CROSS-BORDER DATA FLOWS

23.1 DPA places restrictions on the transfer of personal data outside the European Economic Area (EEA), unless the country or territory involved ensures an adequate level of protection for the rights and freedoms of data

subjects in relation to the processing. If, after careful consideration, it is regarded as essential that the transfer should take place - and if the transfer does not qualify as one of the circumstances when this principle does not apply - the data subject must be notified. Members of staff should note that this restriction has particular implications for international relationships, research projects and information placed onto web sites. This activity should be discussed with the Information Compliance Team to ensure appropriate safeguards and agreements are in place.

24. RESEARCH DATA

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

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

24.1.2 can be held indefinitely; and

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

24.2 There is no blanket exemption from the Data Protection Principles for data provided and/or used for research purposes. Staff will need to assess the legality of processing on each occasion that data are provided for research purposes. Furthermore, researchers will need to ensure that:

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

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

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

24.3 Those conducting research involving the processing of personal data should do so in the context of the University's agreed ethical guidelines, codes of practice and ethics procedures particular to their field of study and Data Protection law.

25. EXAMINATIONS

25.1 Students will be entitled to information about examination marks. However, the University has a longer period to respond to access requests (40 days from the announcement of the results, or five months from the date of the request).

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

26. DISCIPLINE

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

27. POLICY REVIEW

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

28. FURTHER INFORMATION

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

28.2 If you have any queries or concerns, or require further advice, please contact the Information Compliance Team: infocompliance@leedsbeckett.ac.uk or the Data Protection Officer: dpo@leedsbeckett.ac.uk.

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

This policy was approved by the University Secretary on 02 06 2020 and is due for review no later than 01 06 2023.