Data Protection Policy – May 2018 v.02

1. Introduction

1.1. This policy sets out De Montfort University's ('DMU') definition of, commitment to and requirements for the handling of personal data (any information relating to an identifiable person who can be directly or indirectly identified from the data), to support university operations and meet the legislative requirements in accordance with the UK's data protection legislation[1], including the General Data Protection Regulation (GDPR). It sets out the DMU's policy for the adequate protection of personal data throughout its lifecycle, from collection to disposal. This policy should be familiar to all staff dealing with personal information.

1.2. This Data Protection Policy ('DP Policy') provides management direction and support for the management of personal data across the university. This policy has been ratified by the Organisational Leadership Group of the university and forms part of its policies and procedures. It is applicable to, and will be communicated to all staff, students and other relevant parties. This document includes:

1.2.1. The purpose, scope, definitions of the DP Policy.
1.2.2. Responsibility for DP Policy documentation.
1.2.3. Responsibilities for implementing DP Policy and procedures.
1.2.4. References to related documents.

2. Purpose of University DP Policy Documentation

2.1. De Montfort University recognises that efficient management of personal information is necessary to support its core functions, to assist with the effective management of the university, to comply its legal obligations and to provide evidence of such compliance.

2.2. To provide clarity that all DMU staff, including those working for and on behalf of the university, have a responsibility to ensure that personal data is properly managed in compliance with the law.

2.3. To set out that DMU policy documentation should:

[1] The General Data Protection Regulation replaces the Data Protection Act 1998 as of May 25th 2018, but will be superseded, post Brexit, by a new Data Protection Act, which is expected to place GDPR onto the UK statute book. Other relevant legislation includes the Privacy and Electronic Communications Regulations ('PECR') and the EU ePrivacy Regulation.

2.3.1. Present a comprehensive and coherent approach to handling of personal data at a strategic level.
2.3.2. Reflect the objectives of the university by defining expected standards.
2.3.3. Facilitate on-going development, scrutiny and revision of policies at strategic and tactical levels.
2.3.4. Provide guidance or direction to users, administrators and developers of university information systems.
2.3.5. Ensure that the university complies with its legal obligations with regard to data protection law.

3. Scope

3.1. This policy applies to recorded information in any format regarding:

- Living people
- Where they are identifiable from that data
- And where data is held in the EU[2] or
- Where the subjects of the data are EU[3] citizens and
- Where said data is processed by De Montfort University for its own purposes.

Legislative environment

3.2. As of May 25th 2018, the General Data Protection Regulations will apply in the UK. GDPR replaces the European Data Protection Directive with which the Data Protection Act 1998 was the UK's compliance. The Data Protection Bill[4] currently before Parliament will bring GDPR into British law, but is subject to change. The Bill is expected to become law before the UK exits from the European Union, after which there will be a new Data Protection Act.

3.3. The supervisory authority for the university will be the Information Commissioner (ICO).

4. Definitions

4.1. This document uses the definitions as set out in Appendix A.

5. Data Protection Principles

5.1. All processing of personal data must be in accordance with the principles relating to processing of personal data as set out in Article 5 of the GDPR, as listed in Appendix A.

6. Right of Data Subjects

6.1. DMU will ensure that the rights of Data Subjects, as defined in Articles 12-22 of GDPR, are observed at all times. The rights are listed in Appendix A.

2 and post-Brexit, the EU and the UK
3 as above
4 https://services.parliament.uk/bills/2017-19/dataprotection.html

7. Lawful bases for processing

The university will ensure that it ensures that it has determined and recorded a lawful basis for processing under Article 6 of the GDPR (Lawfulness of Processing) and, where applicable, a lawful basis under Article 9 of GDPR (Processing of special categories of personal data), and as listed in Appendix A.

8. Data Protection Officer

8.1. DMU is defined as a Public Authority for the purposes of the GDPR. This necessitates the mandatory appointment of a Data Protection Officer ('DPO'), who must be involved properly and in a timely manner, in all issues that relate to the protection of personal data and adequately resourced to carry out their mandated tasks. The DPO is responsible for providing advice to DMU as to how it might meet its requirements under GDPR.

8.2. The DPO's contact details must be publically accessible, and the Officer must have regard to the risks associated with processing operations, taking into account the nature, scope, context and purposes of processing.

8.3. The tasks of the DPO are set out in Appendix C.

9. Records of data processing activities

9.1. DMU is required to collect records of processing. These set out the purposes for which personal data is processed and the lawful basis for that processing, and will identify all relevant policies and processes relating to that task. Where a breach of data protection occurs that requires notification to the ICO under GDPR, the record of processing forms part of the notification.

9.2. DMU will maintain an Information Asset Register ("IAR") to record the location of Information Assets and associated metadata to enable ownership, purpose, retention and access to be determined. A single asset may be used for multiple

[5] This is the proposal set out in Clause 6 of the Data Protection Bill.

purposes.

9.3. DMU collects records of consents for processing, and records of any exercise of Data Subject rights.

9.4. All records are maintained in compliance with the university's Records Management Policy, Records Retention and Deletion Policy and Information Handling Policy.

10. Privacy Notices

10.1. DMU will ensure that Privacy Notices are provided to Data Subjects for all processing of data. Categories of Data Subjects are as follows:

- Prospective students
- Current student
- Alumni & former students
- Prospective staff
- Current staff
- Former staff
- Third parties (including, but not limited to, contractors & partner organisations)

10.2. Privacy Notices must be provided to Data Subjects, supplying the information required under Articles 12, 13 and 14 of GDPR. Where data collection is direct from the Data Subject, Privacy Notices should be presented at the point of data collection whenever possible. Where data collection is not direct from the Data Subject, they must be provided within one month and:

- If data is used to communicate with the individual, when the first communication takes place or
- If disclosure to another recipient is envisaged, at the latest, before the data is disclosed

10.3. Privacy Notices will set out the purposes and legal basis for any processing, the retention period of the data, whether the data is shared with third parties, the Data Subject's rights, and any other obligations placed upon it under GDPR. The Privacy Notice Procedure sets out how DMU provides Privacy Notices.

11. Disposal of Personal Data

11.1. DMU will adopt mechanisms to allow it to securely dispose of personal data in accordance with the university's records retention schedule.

12. Privacy by Design

12.1. DMU will adopt policies, procedures and design principles procedures, including Data Privacy Impact Assessments and enterprise architectural standards, to ensure that the privacy and security of personal data is considered at the earliest

possible stage of processing. These will include the use of pseudonymisation and anonymisation to prevent the identification of individuals.

12.2. DMU will consider the security of personal data in its control at all times, and will ensure the confidentiality, integrity and availability of personal data through appropriate controls and organisational measures.

13. Data Privacy Impact Assessments

13.1. DMU will ensure that all processing of personal data is been subject to a Data Privacy Impact Assessment6 ('DPIA'), formally known as a Privacy Impact Assessment ('PIA'). The DPIA will identify privacy and security risks to personal data and generate potential mitigations. Mitigations will be appraised against risk criteria and once identified and approved, actions will be carried out.

13.2. DPIA screening is required to check existing processing is complaint, and again as new processing occurs, or processing changes, with full DPIAs as indicated by the screening responses. A Data Privacy Impact Assessment Procedure will set out how DMU undertakes DPIAs.

13.3. The DPIA procedure will be mandatory for all formal projects and will be a requirement of the university's project management methodology.

14. Data Breach Process

14.1. DMU will ensure that a procedure for investigation all breaches of data protection legislation is maintained and followed at all times. Breaches to be covered by the procedure include:

- personal data breach (security breach)
- breaches of lawful processing
- breaches relating to a Data Subject's rights.

14.2. A personal data breach is defined as an incident that "leads to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data".

14.3. A breach of lawful processing occurs when there is no lawful basis for processing personal data. A breach occurs even when no harm is occasioned by the Data Subject.

14.4. A breach of a Data Subject's rights occurs when a Data Subject is prevented from enforcing one of the rights of a Data Subject (see Appendix A) through the

6 Formally known under DPA as a "Privacy Impact Assessment"; the DPIA places greater emphasis on information security in addition to privacy.

data controller's action or inaction.

14.5. All personal data breaches must be notified to the Data Protection Officer as soon as possible after discovery. The university's Data Protection Breach procedure establishes the nature and cause of the breach, the risk to affected parties, including DMU, and will identify mitigating actions.

14.6. Where a risk to the rights and freedoms of an individual is identified as a consequence of a personal data breach, DMU will notify the Information Commissioner of the breach as soon as possible within 72 hours of becoming aware of the breach. Where a high risk to the rights and freedoms of an individual is identified, DMU will notify affected Data Subjects of the breach. The Personal Data Breach Procedure will set out how DMU investigates personal data breaches.

15. Training and Awareness

15.1. DMU will provide adequate training to ensure that staff are aware of their responsibilities under GDPR. All staff will be required to undertake e-learning with a test for comprehension repeated every two years.

16. Subject Access Requests

16.1. DMU will adopt a process that allows Data Subjects to request their own personal data. The process will be free of charge and a response will be provided within one calendar month of receipt of the request. Data Subject Access Requests will be overseen by the Information Governance Manager, but it will be the responsibility of the business area holding the data to locate and extract data relevant to a request in an electronic form (unless otherwise specified) and identify third party data that requires redaction. A Data Subject Access Request Procedure.

17. Contract Compliance

17.1. All contracts will ensure that where personal data is to be processed by a data processor that full instructions as to the permissible processing are communicated to the processor.

17.2. All contracts will ensure that where personal data is to be processed in common by more than one data controller that the respective responsibilities of each controller to achieve compliance and maintain the rights of Data Subjects is clearly established and communicated to the Data Subject via a Privacy Notice.

17.3. All contracts will ensure that where personal data is to be processed, adequate organisational and technical measures are in place to protect the data at all times, including, where transfers occur to countries outside the EU, that

adequate safeguards are employed.

17.4. Legal Services should be consulted on all contractual compliance matters, including those set up by other part of DMU including, but not limited to, Procurement.

18. Direct Marketing

18.1. Consent is the only basis for marketing to an individual where marketing is electronic (email, telephone or direct messaging via social media (AKA 'over the top' marketing)).

18.2. Postal marketing does not require the consent of the individual.

18.3. Consents must be collected by a clear, unambiguous, positive indication of agreement, unless the marketing directly relates to an activity for which a Data Subject has given their consent, in which case a soft-consent can be inferred for related activities (e.g. if a potential applicant requests a prospectus, it would be legitimate to send that individual marketing materials relating to Open Days etc. A Data Subject should be aware that if they are likely to receive marketing materials on related materials at the point of the original consent).

18.4. Each marketing activity requires a separate consent.

18.5. Consents for telephone marketing should be marked as overriding any subscription to the Telephone Preference Society, but only for the specific marketing activity or activities consented to.

18.6. Any department or section that uses personal data for direct marketing purposes must inform Data Subjects of this at the time of collection of the data.

18.7. Individuals must be provided with a simple means by which to object to the use of their data for direct marketing purposes on each communication (e.g. an opt-out link on an email).

19. References to other legislation/standards

- Relevant legislation and Codes of Practice includes but is not restricted to:
- EU ePrivacy Regulation
- Freedom of Information Act 2000
- Human Rights Act 1998
- Disability Discrimination Act 1995
- Privacy and Electronic Communications Regulations 2003
- Regulation of Investigatory Powers Act 2000
- Limitations Act 1980

20. References to Strategic Level Policy Sub-Documents

- Principal Information Technology and Security Policy
- Information Handling Policy
- Records Retention & Disposal Policy
- Records Management Policy
- User Management Policy
- Use of Computers Policy
- System Planning and Management Policy
- Mobile Computing Policy

21. Document Approval

- Approved by:
- Approved Date:
- Review Date:
- Reviewer:

22. Document History

- 22nd November 2017 – Draft 1 Fraser Marshall
- 11th December 2017 – Draft 2 Fraser Marshall
- 08th January 2018 – Draft 3 Fraser Marshall
- 24th January 2018 – Draft 4 Fraser Marshall
- 19th February 2018 – Draft 5 Fraser Marshall
- 07th March 2018 – Draft 6 – Fraser Marshall

Appendix A – Definitions, Principles, Lawful basis and Data Subject Rights

This appendix provides a list of definitions as used in the Data Protection Policy, the data protection principles, the legal basis for processing both personal and special category data and the rights of the Data Subject. These are based on current data protection legislation, principally the GDPR.

Definitions:

Personal Data – recorded personal information in any format 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
- one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

Special Category Data - Special Category Data are subject to stricter controls for processing. They include recorded personal information in any format revealing:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- the processing of genetic data
- biometric data for the purpose of uniquely identifying a natural person
- data concerning health or data concerning a natural person's sex life or sexual orientation
- Data relating to criminal offences

Data Controller - Any organisation who makes decisions with regard to particular personal data, including decisions regarding the purposes for which personal data are processed and the way in which the personal data are processed. For the purposes of this policy, this is DMU, unless otherwise specified.

Data Processor – Any organisation that processes personal data solely for the purposes of DMU. Data Processors must be appraised for GDPR compliance and instructed by DMU as to the nature of the processing they will undertake.

Data Subject - Any living individual who is the subject of personal data held by an organisation.

Processing - Any operation related to organisation, retrieval, disclosure and deletion of data and includes:

- obtaining and recording data
- accessing, altering, adding to, merging, deleting data
- retrieval, consultation or use of data
- disclosure or otherwise making available of data.

Third Party - Any individual/organisation other than the Data Subject, the data controller (DMU) or its agents .

Data Protection Principles:

All processing of personal data must be in accordance with the principles relating to processing of personal data as set out in Article 5 of the GDPR:

a) processed lawfully, fairly and in a transparent manner in relation to the Data Subject ('lawfulness, fairness and transparency');
b) 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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
d) 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 ('accuracy');
e) 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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the Data Subject ('storage limitation');
f) 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 ('integrity and confidentiality').
g) Accountability

Conditions for Lawful Processing:

The lawful basis for processing personal data are as follows:

a) Consent
b) processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract; processing is necessary for compliance with a legal obligation to which the controller is subject;
c) processing is necessary in order to protect the vital interests of the Data Subject or of another natural person (essentially, this relates to processing of personal data in life and death situations);
d) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
e) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of personal data, in particular where the Data Subject is a child.

Where special category data is processed, an additional processing condition is required from the following list:

a) the Data Subject has given explicit consent to the processing of those personal;
b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the Data Subject in the field of employment and social security and social protection law;
c) processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent;
d) processing relates to personal data which are manifestly made public by the Data Subject;
e) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
f) processing is necessary for reasons of substantial public interest;
g) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;
h) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices;
i) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes;

The Rights of the Data Subject

Data Subjects have the following rights:

- **The right to be informed** - concerns DMU's obligation to provide 'fair processing information', through a privacy notice which is concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children. Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.
- **The right of access** - Individuals have the right to access their personal data and supplementary information. They are entitled to be aware of and verify the lawfulness of the processing.
- **The right to rectification** – where data is incorrect or incomplete, Individuals are entitled to have it corrected. Corrections must be passed to any parties with whom the data has been shared. This must be done without delay, and no later than one month. This can be extended to two months with permission from the DPO.
- **The right to erase** – AKA 'the right to be forgotten'. Individuals can request the deletion or removal of personal data where there is no compelling business reason for its continued processing.
- **The right to restrict processing** – Individuals can demand that processing is suspended while inaccurate data is amended, or where they have made any objection to the processing, where the processing is unlawful and the individual opposes erasure or where DMU is seeking to destroy or erase the data but the data is required by the individual in order to take or defend legal action. We must comply with any request to restrict, block, or otherwise suppress the processing of personal data.
- **The right to data portability** – Individuals can request a copy of their data for their own purposes:
  - The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.
  - It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. We must provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.
- **The right to object** – Individuals can object to any processing based on legitimate interest or the performance of a public interest task, and if in dispute over whether the processing is harmful have a right to have processing halted until a resolution is agreed. The right to object to marketing is key, and all marketing materials must give an individual the means by which to opt out of receiving future marketing. We must respect the right of an individual to object to processing their data for scientific and historical research and statistics. However, a request can be refused if to comply would render impossible or seriously impair the achievement of the specific purposes.
- **Rights in relation to automated decision making and profiling** – Where computer logic results in actions in respect of a person (e.g. send all students matching a particular criteria one letter and everyone else gets another letter), Data Subjects have a right to demand human intervention or to challenge a decision and a right to investigate whether the processing is legal.

Appendix B - Common Sources of Personal Data

The following are some of major repositories of personal data in the university. The university is collecting an information asset register in order to hold a corporate record of where data is held. This will be accessible by request after May 25th 2018 from the Information Governance Manager or the Data Protection Officer.

- HR records
- Finance System
- Student Lifecycle Management
    - Plus legacy systems (PSE, QLS, QLF) and any archiving systems relating to the above stores
- Faculty offices - applications
- Disability Team Records
- Counselling and Welfare Team Records
- CRM
- Job applications
- Disciplinary records
- Research data
- Security records
- Student complaints
- Prospectus requests
- Open Day applications
- ADMIS records
- DMU International

Appendix C – The Tasks of the Data Protection Officer

The following are the minimum tasks that a DPO should be assigned. The DPO must have regard to the risks associated with processing operations, taking into account the nature, scope, context and purposes of processing.

- informing and advising DMU, any data processor engaged by the university, and any employee of the controller who carries out processing of personal data, of that person's obligations under this Part,
- providing advice on the carrying out of a data protection impact assessment under section 62 and monitoring compliance with that section,
- co-operating with the ICO and other regulatory authorities,
- acting as the contact point for the ICO on issues relating to processing, including in relation to the consultation mentioned in section 63, and consulting with the ICO, where appropriate, in relation to any other matter,
- monitoring compliance with the university's policies in relation to the protection of personal data, and monitoring compliance by DMU with their obligations in respect of
- their general obligations to data protection by design and default
- where they are controllers, joint controllers or processors
- any obligations relating to processing
- keeping records of processing activities and other mandated records
- Co-operating and consulting with the ICO
- carrying out data protection impact assessments
- upholding the obligations relating to security
- handling breaches and communication to the ICO and Data Subjects as required.

In relation to the policies mentioned above, the DPO's tasks also include assigning responsibilities under those policies, raising awareness of those policies, training staff involved in processing operations, and conducting audits required under those policies.