1.1. To set out De Montfort University's (DMU's) policy for the secure processing of personal data for which DMU is the data controller.

1.2. To ensure that DMU complies with relevant privacy laws, most notably the Data Protection Act (DPA 2018) the UK General Data Protection Regulation (UK GDPR), the Privacy & Electronic Communications Regulations (PECR).,

1.3. To ensure that DMU processes personal data fairly and lawfully, as set out by the seven key principles of the UK GDPR.

1.4. To ensure that DMU staff, governors, contractors and other third parties working for or on behalf of DMU, are aware of their responsibilities for the protection of personal data.

2.1 Personal data

2.1.1 The UK GDPR defines personal data as information from which a natural (living) person can be identified, either directly or indirectly.

2.1.2 This policy covers personal data for which DMU is the data controller. Under data protection law, the data controller is the body that legitimately determines the purpose and means of the processing.

2.2 DMU staff

This policy is applicable to all DMU employees, and all staff working for or on behalf of DMU, whether directly employed or on temporary contracts including governors, contractors, students undertaking placements or internships at DMU, and other third parties. It is also applicable to students conducting research as part of their studies.

3.1 There must be a lawful basis for the processing

3.1.1 One lawful basis under Article 6 of the UK GDPR (lawfulness of general processing) must be defined and, where applicable, one lawful basis under Article 9 (to process special categories of personal data) must also be defined.

3.1.2 To process criminal offence data, one lawful basis under Article 6 must be defined, and a condition for processing under the DPA 2018 must also be met. Under the DPA 2018, criminal offence data is the equivalent of special category data.

3.1.3 The lawful basis must be clearly documented in the 'Record Of Data Processing Activities' and an explanation as to how the processing complies with the law included in the 'Privacy Notice'.

3.2 Appropriate documentation must be maintained

3.2.1 ***Record Of Data Processing Activities (ROPA)***

The ROPA is overseen by the Information Governance Team.

Each Faculty or Directorate (or sub-team within where this is appropriate) must maintain a 'ROPA. This must include:

- the purpose of the processing
- categories of individuals whose personal information is processed, e.g. staff, students (prospective, current, alumni), partners
- categories of personal data, i.e. whether it is falls under general processing alone or includes special category, or criminal offence data.
- The source(s) of the personal data
- the lawful basis/bases for the processing under the UK GDPR and, for criminal offence data, the condition relied upon under the DPA 2018
- any transfers of personal data outside the UK and to countries not deemed adequate by the UK, and what safeguards are in place where such transfers occur
- how long personal data is retained for (or link to the DMU's retention policy), or how retention is determined
- the location of the information (where it is stored)
- a description of the technical and organisational security measures (or hyperlink to relevant policies and procedures).
- where consent is the lawful basis, how this is recorded
- information required for (or link to) privacy notice(s)

3.2.2 ***Privacy Notice***

DMU will publish or make available a Privacy Notice(s) that is understandable by all stakeholders. The privacy notice will be formally reviewed every two years unless there is change to legislation or guidance that requires more immediate changes., considering feedback from interested parties. The privacy notice must include:

- the purpose(s) of the processing
- the lawful basis/bases for the processing
- the rights of individuals under the UK GDPR

- the source(s) of the personal data that are processed
- the existence of automated decision making or profiling
- who the personal data may be shared with (third parties)
- how we keep personal data secure
- how to make a subject access request and exercise other rights
- that DMU is the data controller
- contact details of DMU's Data Protection Officer (DPO) (DPO@dmu.ac.uk)

3.2.3 ***Information Asset Register (IAR)***

An IAR is an information security requirement. The IAR is overseen by the Information Governance Team The IAR should include:

- the name of the asset
- a description of the asset, i.e. the type of information and what it does (e.g. payroll system)
- the name of the system or database upon which the asset is stored
- where applicable, the system administrator
- the volumes of records held on the system or database
- the location of the asset
- the job title of the identified information asset owner
- the retention period of the information asset
- who has access to the information asset (for example, which teams), including third parties
- the value of each asset (i.e. The risk to the university if the asset was lost, destroyed, compromised or accessed by unauthorised individuals.)

3.3 Data Protection Officer (DPO)

DMU has an appointed DPO. The DPO is responsible for providing advice to DMU and monitoring its compliance with data protection laws. The DPO will be adequately resourced to carry out their duties and responsibilities.

The DPO is a statutory post. The DPO's contact details are included in the Privacy Notice. The DPO can be contacted at DPO@dmu.ac.uk.

Day to day adherence to data protection is overseen by the Information Governance Team consisting of the Information Governance Manager, Records Manager and Information Governance Officers. The Information Governance Team can be contacted at dataprotection@dmu.ac.uk

Both the DPO and the Information Governance Team work closely with the university's Senior Information Risk Owner, who is a member of the university leadership board, and colleagues in ITMS.

3.4

and similar requests. to be responded to within one calendar month although this time period can be extended by a further two months in the case of complex requests.

3.5 Data Protection Impact Assessment (DPIA)

3.5.1 A DPIA is a process to help the owner of the process to identify and minimise the data protection risks inherent in any processing of personal data. UK GDPR makes it a requirement to undertake a DPIA where processing is likely to result in a high risk to the rights and freedoms of natural persons

3.5.2 A DPIA should be carried out at the earliest opportunity so that privacy is 'by design and default'. A DPIA should be undertaken whenever there is a new processing activity being proposed, or where there is a change to existing processing activities which may impact on privacy. DPIAs should be conducted by the person responsible for the processing or a designated deputy

3.5.3 A DPIA Screening Checklist and DPIA template are made available on the Intranet or from the Information Governance Team. Checklists and full DPIAs must be formally approved by the Information Governance Team.

3.5.4 Consideration will be given to the use of pseudonymisation and anonymisation where this security measure can be practically implemented without compromising the purpose of the processing.

3.6 Personal Data Breach reporting

3.6.1 DMU has a responsibility to notify the ICO within 72 hours where a personal data breach is likely to result in a risk to the rights and freedoms of natural persons. Information security incidents involving personal data, including near misses, will be logged and investigated by local management in cooperation with the Information Governance team.

3.6.2 All incidents will be immediately reported to the DPO and the Information Governance Team.using the following email addresses: . DPO@dmu.ac.uk and dataprotection@dmu.ac.uk

3.6.3 A decision will be taken by the DPO and Information Governance Manager as to whether a breach reaches the threshold for notification to the Information Commissioner's Office.

3.6.4 Personal Data Breaches will be monitored by the Information Governance and Cyber Security Committee (IGCSC) and will be reported to the University Leadership Board as appropriate. The university regularly reviews breaches to identify specific risks in order to reduce future incidents occurring and to inform best practice.

3.6.5 The proactive reporting of information security concerns to the

Information Governance Team is encouraged. These may relate to physical or electronic records.

3.7 Staff training

3.7.1 DMU will provide adequate staff training to ensure that all staff are aware of their responsibilities for data protection and information security.

3.7.2 Data [illegible]

The IT Governance & Security Manager is responsible for managing information security incidents, and for mitigating information security incidents and risks.

The Information Governance Manager is responsible for reviewing and updating this policy and for managing SARs and associated Data Subject requests, approving DPIAs, the investigation of personal data breaches, and providing guidance on data protection issues when requested as well as providing proactive guidance and training on matters connected to Data Protection.

The Information Governance team will respond to SARs and associated Data requests, assist colleagues in the completion of DPIAs, investigate personal data breaches and provide training and guidance on data protection issues as required.

- Privacy & Electronic Communications Regulations 2003
- Human Rights Act 1998 (Article 8)
- Common law duty of confidence
- Computer Misuse Act 1990
- Regulation of Investigatory Powers Act 2000
- Limitations Act 1980
- ICO Code of Practice for anonymisation
- Rehabilitation of Offenders Act 1974
- Internal guidance and training documents

- Appropriate policy document for the processing of special categories of personal data and personal data about criminal convictions and offences. Statutory Requests for Information Policy
- Principal information technology and security policy
- Information handling policy
- Records retention & disposal policy
- Records management policy
- Records Retention Schedule
- User management policy
- Use of computers policy
- Mobile computing policy
- System planning and management policy
- Human resources security policy
- Access control policy

Version No:	Supersedes	Author	Publication Date	Data of next review	Classification
V3	V2	Information Governance Manager			

			Governance Manager	2022	2023	