Data Protection Policy

1. Purpose of the policy

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 General Data Protection Regulation (GDPR), and 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 GDPR.

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

2. Scope and applicability

2.1 Personal data

2.1.1 The 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 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, including governors, contractors and other third parties.

3. Policy

3.1 There must be a lawful basis for the processing

3.1.1 One lawful basis under Article 6 of the 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***

Each department must maintain a 'Record of data processing activities'. 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 lawful basis for the processing under the GDPR and, for criminal offence data, the condition relied upon under the DPA 2018
- any transfers of personal data outside the UK and what safeguards are in place
- 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 reviewed at least annually, taking into account 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 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

- 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 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 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. how critical is the asset to the continuation of a business function and how critical is that function?)

3.3 Data Protection Officer (DPO)

DMU has an appointed DPO. The DPO is responsible for providing advice to the DMU and monitoring its compliance with data protection laws. The DPO will be adequately resourced to carry out his or her 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.co.uk.

3.4 Subject Access Requests (SARs)

SARs will be appropriately responded to. The GDPR requires SARS to be responded to within one calendar month.

3.5 Data Protection Impact Assessment (DPIA)

3.5.1 DPIAs will be incorporated into the project management process.

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 repeated whenever there is a change to processing activities which may impact on privacy.

3.5.3 A DPIA Screening Checklist and DPIA template are made available on the Intranet.

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 Incident reporting

3.6.1 Information security incidents involving personal data, including near misses, will be logged and investigated by information governance staff.

3.6.2 Serious incidents will be immediately reported to the DPO.

3.6.3 Incidents will be monitored by the Information Governance Board (IGB) and will be reported to the DMU Governing Body.

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 protection and information security will be included in induction training for new staff.

3.7.3 All staff are required to undertake information governance e-learning, that includes a test for comprehension, at least once every two years.

3.8 Data processor contracts

3.8.1 All contracts with third party data processors will ensure that full instructions as to the permissible processing are included in the contract.

3.8.2 Contracts must stipulate that adequate organisational and technical measures must be in place to protect personal data, and, where transfers occur to countries outside the EU, include that adequate safeguards must be employed (NB: the European Commission provide standard clauses).

3.8.3 Legal Services must formally approve all contract templates.

3.9 Information Sharing Agreements (ISAs)

Where personal data is to be shared with other data controllers, this will be in accordance with an Information Sharing Agreement that will be agreed between all parties to the agreement.

Stand alone ISAs provide a secure framework for the sharing of personal data. They are not binding agreements.

4. Roles and responsibilities

All staff are responsible for the protection of personal data. Staff should ensure that they follow DMU's policies and procedures that relate to the protection of personal data.

The Data Protection Officer (DMO) is responsible for monitoring DMU's compliance with data protection laws, DMU data protection policies and procedures, awareness raising, training and audits.

The Information Security Manager is responsible for managing information security incidents, and for mitigating information security incidents and risks.

The Information Governance Manager is responsible reviewing and updating this policy and for managing SARs.

5. Other laws, regulations, and guidance

- 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

6. Related documents

- Data Protection Reporting Procedure
- Subject Access Request Policy
- Principal information technology and security policy
- Information handling policy
- Records retention & disposal policy
- Records management policy
- User management policy
- Use of computers policy
- Mobile computing policy
- System planning and management policy
- Human resources security policy
- Access control policy

7. Document control

Version No:	Supersedes	Author	Publication Date	Data of next review	Classification
V2	V1	Interim Information Governance Manager	July 2018	July 2019	Public