Data Protection Policy

1. Policy Statement

The Data Protection Act 2018 (DPA18) and the General Data Protection Regulations (GDPR) (collectively "the Regulations") are designed to protect personal data and uphold the rights and freedoms of living individuals. The GDPR is a Europe-wide standard that affects organisations globally that process personal data of EU citizens.

Digital Marketing School (referred in this document as DMS) processes personal data relating to its current, former, and future staff and students; research, academic, and industry contacts; contractors, visitors, and users of all DMS services. DMS is obligated to meet reasonable expectations of privacy by complying with data protection and privacy laws.

DMS is committed to compliance with the Regulations. This document outlines the approach to data protection at DMS to protect personal data and uphold the institution's reputation and security.

The policy sets out:

- How DMS complies with the GDPR principles;
- Responsibilities and accountabilities for data protection;
- Our approach to privacy by design and by default;
- How DMS manages data protection and privacy risks, particularly personal data breaches.

2. Scope

This policy applies to all personal data and special category data processed by DMS and on its behalf, regardless of location. All staff, students, and those acting on behalf of DMS must comply with this Data Protection Policy.

3. Data Protection Principles

The GDPR sets out seven key principles that organisations must follow, which outline the spirit of the Regulations. Compliance with these principles is essential:

Lawfulness, Fairness, and Transparency
DMS must have a lawful basis for processing personal data and must be transparent about its use.

Purpose Limitation
Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner in compatible with those purposes.

Data Minimisation
Personal data must be adequate, relevant, and limited to what is necessary.

Accuracy
Personal data must be accurate and kept up to date.

Storage Limitation
Personal data must not be kept for longer than necessary. Staff should be aware of the retention schedules for the information that they process and ensure that information is not kept for longer than is necessary.

Integrity and Confidentiality
The GDPR requires that there be appropriate technical and organisational security measures in place to protect personal data. The University policies, culture, organisational structures and operating environment promote the confidentiality, integrity and availability of the University's information assets throughout their lifecycle from beginning, through use to end of use.

Accountability
DMS must be able to demonstrate compliance with these principles.

4. Responsibilities of Staff and Students

All staff, including temporary, contractors, and volunteers, and students are responsible for:

- Adhering to this policy and supporting policies;
- Ensuring technical and practical measures are taken to safeguard personal data;
- Ensuring personal data provided to DMS is accurate and up to date;
- Informing DMS of any changes to personal information;
- Ensuring they process personal data lawfully;
- Sharing information only where there is a lawful basis.

DMS, as Data Controller, exercises overall control over personal data processing. The Data Protection Officer monitors compliance advises on obligations, and acts as a contact point for the Information Commissioner's Office (ICO).

5. Rights of Data Subjects

Data subjects have several rights regarding their personal data:

- The right to be informed about its collection and use;
- The right of access to their personal data;
- The right to rectification of inaccurate or incomplete data;
- The right to erasure (right to be forgotten);
- The right to restrict processing;
- The right to data portability;
- The right to object to processing under certain circumstances;
- Rights related to automated decision-making and profiling.

DMS has procedures to manage and monitor individual rights requests, in line with the Subject Access Policy and Individual Rights Policy.

6. Data Sharing

Internal Sharing
Personal data may be shared internally if necessary for the intended purpose or another lawful purpose.

External Sharing
Personal data may be shared with third parties if there is a lawful basis. For routine sharing without a contract, a data sharing agreement is required. For ad hoc requests, ensure identity verification, secure sharing methods, minimal data sharing, and record the decision and actions taken.

International Transfers
Personal data transferred outside the EEA must comply with GDPR Article 46 protections, such as using standard contract clauses.

7. Data Retention

Personal data must be retained only as long as necessary for processing purposes. DMS's Data Retention Schedule outlines retention periods. Staff must follow these schedules and consult with line managers or the Information Governance team for guidance.

8. Compliance

Failure to comply with this policy could result in financial and reputational damage to DMS and disciplinary or legal action against individuals.

Remember: protect the University, protect individuals and protect yourself.

9. Support and Escalation

The Director of DMS, Dr. Mohammad Shafiqul Islam offers advice and guidance on data protection and can be contacted at shafiq@londondms.com.

10. Related Documentation

The following documents are available on the DMS Policy & Procedure pages:

- Appeals and Complaints Policy
- Malpractice, Maladministration and Plagiarism Policy
- Conflicts of Interest Policy
- Equality, Diversity and Inclusion Policy
- Assessment Policy
- Internal Quality Assurance Policy
- Reasonable Adjustment and Special Consideration Policy
- Learner Recruitment and Admissions Policy
- Staff Development Policy
- Blended and Distance Learning Policy