



LUMINA OPEN UNIVERSITY: DATA PROTECTION POLICY

1. Purpose and Scope

The purpose of this Data Protection Policy is to outline how Lumina Open University (hereinafter referred to as “the University”) manages, protects, and processes personal data in compliance with relevant data protection laws and regulations, including the General Data Protection Regulation (GDPR) and other applicable local laws.

The policy applies to all staff, faculty, students, and external contractors who process personal data on behalf of the University. It governs the collection, storage, use, sharing, and disposal of personal data within the University’s operations, including but not limited to data related to students, employees, alumni, and other stakeholders.

2. Data Protection Principles

Lumina Open University adheres to the following principles regarding data protection, as outlined by applicable laws:

- **Lawfulness, Fairness, and Transparency:** Personal data will be processed lawfully, fairly, and in a transparent manner. Individuals will be informed about how their data will be used, and their consent will be obtained when necessary.
- **Purpose Limitation:** Personal data will only be collected for specified, legitimate purposes and not processed further in a manner incompatible with those purposes.
- **Data Minimization:** The University will collect and process only the minimum amount of personal data necessary for the specified purposes.
- **Accuracy:** The University will take reasonable steps to ensure that personal data is accurate, complete, and up-to-date.
- **Storage Limitation:** Personal data will be kept for no longer than is necessary to fulfill the purposes for which it was collected and processed. Once no longer needed, data will be securely disposed of.
- **Integrity and Confidentiality:** The University will implement appropriate technical and organizational measures to ensure the security, confidentiality, and integrity of personal data.
- **Accountability:** The University will be accountable for its processing of personal data and will implement measures to demonstrate compliance with data protection laws.

3. Types of Personal Data Collected

The University collects and processes various types of personal data, including but not limited to:

- **Student Data:** Name, contact information, date of birth, academic records, financial information, attendance, and any other personal details provided for admission or academic purposes.
- **Employee Data:** Name, contact details, job role, employment history, salary, and other employment-related information.
- **Alumni Data:** Contact details, academic records, and any other information relevant to alumni relations and communication.
- **Research Data:** Personal information relating to research participants, including demographic details and survey responses, where applicable.
- **External Stakeholder Data:** Contact information for contractors, partners, suppliers, or other external parties.

4. Lawful Bases for Processing Personal Data

The University processes personal data based on one or more of the following lawful bases, as per data protection laws:

- **Consent:** The individual has given explicit consent for their personal data to be processed for specific purposes (e.g., subscribing to newsletters or marketing materials).
- **Contractual Necessity:** Processing is necessary for the performance of a contract (e.g., enrollment in academic programs or employment contracts).
- **Legal Obligation:** Processing is required to fulfill legal obligations (e.g., tax reporting, government compliance).
- **Legitimate Interests:** Processing is necessary for the legitimate interests of the University or a third party, provided this does not override the rights and freedoms of the individual.
- **Vital Interests:** Processing is necessary to protect the life of an individual (e.g., in cases of medical emergencies).
- **Public Task:** Processing is necessary to carry out an official function or task in the public interest, such as academic accreditation or regulatory requirements.

5. Rights of Data Subjects

Under applicable data protection laws, individuals whose personal data is processed by the University have the following rights:

- **Right to Access:** Individuals have the right to request access to the personal data the University holds about them.
- **Right to Rectification:** Individuals can request the correction or update of inaccurate or incomplete personal data.
- **Right to Erasure (Right to be Forgotten):** In certain circumstances, individuals can request the deletion of their personal data.
- **Right to Restriction of Processing:** Individuals may request that the processing of their personal data be limited in certain situations.
- **Right to Data Portability:** Individuals have the right to receive their personal data in a structured, commonly used format and transfer it to another data controller.

- **Right to Object:** Individuals can object to the processing of their personal data on grounds related to their particular situation, particularly in cases of direct marketing or profiling.
- **Right to Withdraw Consent:** Where processing is based on consent, individuals can withdraw their consent at any time, and the University will stop processing their personal data for that purpose.

6. Data Security Measures

Lumina Open University is committed to ensuring the security of personal data and has implemented appropriate technical and organizational measures to protect data from unauthorized access, alteration, disclosure, or destruction. These measures include, but are not limited to:

- **Encryption** of personal data where necessary.
- **Access Control** ensuring that only authorized personnel have access to personal data.
- **Regular Audits** and monitoring to ensure compliance with this policy and identify potential vulnerabilities.
- **Data Backup** systems to protect against data loss in the event of system failures or disasters.

7. Data Sharing and Third-Party Processing

Lumina Open University may share personal data with third parties only when it is necessary to fulfill contractual obligations or comply with legal requirements. The University will ensure that any third parties involved in the processing of personal data have appropriate data protection measures in place and will enter into Data Processing Agreements (DPAs) where applicable.

Data may be shared with:

- **Service Providers:** External vendors or contractors who support the University's operations (e.g., IT service providers, payment processors, research collaborators).
- **Government Agencies:** For purposes such as compliance with tax laws or educational regulations.
- **Accrediting Bodies:** In compliance with academic or professional accreditation requirements.

In all cases, the University will ensure that third-party processors adhere to strict data protection standards and will monitor their compliance.

8. Data Retention and Disposal

Personal data will only be retained for as long as necessary to fulfill the purposes for which it was collected, or as required by law. After this period, data will be securely disposed of or anonymized to ensure that it cannot be reconstructed or used inappropriately.

9. Training and Awareness

The University will ensure that all staff members, especially those handling personal data, receive regular training on data protection principles and practices. This will include training on how to manage personal data securely, recognizing data breaches, and responding to data subject requests.

10. Data Protection Officer (DPO)

Lumina Open University has appointed a Data Protection Officer (DPO) to oversee compliance with this policy and data protection laws. The DPO is responsible for:

- Monitoring and ensuring compliance with data protection laws.
- Providing advice and guidance on data protection matters.
- Handling data subject requests and complaints.
- Conducting regular audits of data processing activities.

The DPO can be contacted directly through the University's official communication channels.

11. Reporting Data Breaches

Any data breaches or security incidents that could potentially compromise the security of personal data must be reported immediately to the Data Protection Officer. In the event of a breach, the University will investigate, mitigate, and notify affected individuals and the relevant authorities as required by law.

12. Compliance and Review

This Data Protection Policy will be reviewed regularly to ensure it remains in compliance with applicable laws and reflects the best practices in data protection. Any updates or changes to the policy will be communicated to all relevant stakeholders.

13. Conclusion

Lumina Open University is committed to upholding the highest standards of data protection and ensuring the privacy and security of personal data entrusted to it. This policy ensures that personal data is processed responsibly, legally, and ethically, safeguarding the rights of individuals while supporting the University's mission of providing accessible, high-quality education.