MISR UNIVERSITY FOR SCIENCE AND TECHNOLOGY
جامعة مصر للعلوم والتكنولوجيا

PERSONAL DATA PROTECTION POLICY
For Faculty Members, Students & Staff

Policy Issue	2025 / 2026
Approved By	Chief Information Technology Officer (CITO)
Supervising Authority	Chief Information Technology Officer (CITO)
Review Cycle	Annual

Article 1 — Introduction & Purpose

Misr University for Science and Technology is a leading academic institution committed to protecting the privacy and personal data of all its affiliates, in accordance with the highest academic and professional standards. This Policy establishes the regulatory and legal framework governing the collection, processing, storage, and disclosure of personal data, thereby ensuring the safety and protection of rights of the entire University community.

The provisions of this Policy apply to all entities within the University that handle personal data, including: senior management, colleges, academic departments, student affairs directorates, human resources, information technology, affiliated hospitals, and all authorised external parties.

Article 2 — Scope of Application

A. Categories Covered

- Faculty members and teaching assistants at all academic ranks.
- Undergraduate, postgraduate (Master's and Doctoral) students.
- All students who have applied for enrollment (undergraduate, postgraduate, and doctoral) whose admission procedures have not yet been completed.
- Administrative, technical, and support staff.
- Visiting researchers, visiting professors, and trainees.
- Applicants for admission or employment, and alumni.
- Service suppliers and external contractors affiliated with the University.

B. Geographical & Technical Scope

- All University premises, campuses, and research centres.
- Electronic systems and digital platforms owned by the University.
- Remote work arrangements and officially approved cloud-based systems.
- Any processing occurring outside the campus under formal authorisation.

Article 3 — Categories of Personal Data Collected

Category	Examples of Data	Primary Purpose
Identity Data	Name, national ID number, ID photograph, date of birth	Registration, identity verification, and employment
Contact Data	Email address, home address, telephone numbers	Official communication and sending notifications
Academic Data	Grades, academic records, educational plans	Assessment and academic development
Financial Data	Fee data, salaries, grants and bonuses	Financial obligations and payroll
Technical Data	IP addresses, login records, cookies	System security and network monitoring
Sensitive Data	Health data, individuals with special needs	Providing care and necessary accommodations

Article 4 — Data Processing Principles

Governing Principles

- Lawfulness, Legal Controls & Transparency: Data is processed only for legitimate purposes and with the knowledge of the data subject.
- Purpose Limitation: Data is collected for specified, explicit, and legitimate purposes only.
- Data Minimisation: Only data strictly necessary to achieve the stated purpose is collected.
- Accuracy & Currency: The University ensures data is accurate and regularly updated.
- Storage Limitation: Data is not retained longer than necessary to fulfil the stated purpose.
- Integrity & Confidentiality: Data is protected against unauthorised access, loss, or damage.
- Accountability: The University appoints a Data Protection Officer and maintains processing records.

Article 5 — Rights of Data Subjects

The University guarantees the following rights to all persons covered by this Policy:

Right	Details & Mechanism
Right of Access	Request a complete copy of your data held by the University within 30 working days.
Right to Rectification	Request correction of any inaccurate or incomplete data upon discovery.
Right to Erasure	Request deletion of your data when the purpose lapses or consent is withdrawn, subject to legal retention obligations.
Right to Restriction	Request restriction of data processing in specific cases and during appeal or review periods.
Right to Object	Object to the processing of data for marketing or scientific research purposes without consent.
Right to Data Portability	Obtain your data in an electronic format transferable to another organisation upon request.
Right to Withdraw Consent	Withdraw consent at any time without affecting the lawfulness of processing prior to withdrawal.

Article 6 — Security & Technical Protection Safeguards

Technical Measures

- Data encryption using AES-256 standard at rest and TLS 1.3 protocol in transit.
- Multi-Factor Authentication (MFA) on all sensitive systems.
- Role-Based Access Control (RBAC) with the principle of least privilege.
- Continuous 24/7 security monitoring and real-time threat detection.
- Periodic encrypted data backups with regular restoration testing.
- Periodic penetration tests and annual independent security audits.

Organisational Measures

- Regular awareness and training programmes for all staff on data protection.
- Mandatory confidentiality agreements for all who handle personal data.

- Clean Desk & Clear Screen Policy enforced across all workstations.
- Procedures to verify the data processing practices of external service providers.

Article 7 — Data Retention & Disposal

Type of Data	Retention Period	End-of-Retention Action
Student academic records	Study period + 50 years	Secure archiving per Document Management Regulations
Employee files	Service period + 10 years	Certified secure deletion with a formal disposal record
Technical access logs	12 months	Automatic deletion upon expiry
Financial data	10 years	Encrypted archiving per Financial Law
Data of unsuccessful applicants	1 year	Secure deletion upon expiry
Security camera footage	90 days	Automatic overwrite

Article 8 — Data Breach Response Procedures

In the event of any actual or suspected personal data breach, the University follows the procedures below:

- Discovery & Reporting: Any person who discovers a breach must immediately notify the Information Security team via the dedicated channel (info@must.edu.eg).
- Containment (within 1 hour): Isolate affected systems, restrict access, and collect digital evidence.
- Assessment (within 24 hours): Determine the scope of the breach, the type of data affected, and the number of individuals impacted.
- Notification (within 72 hours): Notify the relevant regulatory authorities in accordance with applicable legal requirements.

- Notifying Affected Individuals: Notify affected data subjects without delay through appropriate means.
- Investigation & Remediation: Conduct a thorough investigation and apply the necessary corrective measures.
- Documentation & Reporting: Produce complete documentation of the incident and a final report with improvement recommendations.

Article 9 — Sharing Data with Third Parties

The University does not share personal data with external parties except in the following cases:

- Compliance with applicable legal, regulatory, and judicial requirements.
- Service delivery by external providers bound by approved data processing agreements.
- Academic accreditation by internationally licensed bodies under confidentiality agreements.
- Joint scientific research with partner universities under documented data-sharing agreements.
- Medical emergencies to protect human life, using the minimum data strictly necessary.

All external service providers are required to sign a Data Processing Agreement in accordance with the University's approved template and are subject to periodic security assessments. No data may be transferred outside the jurisdiction except under appropriate safeguards in accordance with applicable legislation.

Article 10 — Roles & Responsibilities

Entity / Role	Key Responsibilities
Data Protection Officer (DPO)	Oversee compliance, receive complaints, liaise with regulatory authorities, and review policies.
IT Directorate	Implement technical security safeguards, manage access controls, and respond to security incidents.
Staff Affairs & Human Resources	Manage employee files, verify identities, and conduct privacy training.

Student Affairs & Admissions	Protect academic records and handle student data access requests.
Faculty Members	Comply with student data protection policies in research, teaching, and assessment.
All Staff	Report breaches, maintain confidentiality, and adhere to data security procedures.

Article 11 — Policy Violations & Sanctions

Intentional or negligent violation of this Policy constitutes a disciplinary offence, resulting in the following measures:

- First Violation (unintentional): Written warning with mandatory data protection retraining.
- Repeated or Negligent Violation: Formal disciplinary proceedings that may lead to suspension from work.
- Serious or Intentional Violation: Referral to the Disciplinary Board, potentially resulting in contract termination.
- Criminal Violations: Referral to the competent judicial authorities in accordance with applicable law.

This Policy does not constitute a barrier to any legal rights of affected individuals to seek recourse through the courts or competent regulatory authorities.

Article 12 — Contact & Complaints

To exercise your rights or report any concerns relating to the protection of your data, please contact us via:

Contact Method	Details
Email	info@must.edu.eg
Website	www.must.edu.eg/
Data Protection Officer's Office	Media Building, Ground Floor, Network Administration Office — Main Campus
Response Period	30 working days from receipt of the completed request

Official Endorsement

Chief Information Technology Officer (CITO)
Signature:
Date: