Personal Data Protection Policy

First: Introduction

In line with October 6 University's commitment to implementing the highest standards of institutional governance, protecting individual privacy, and promoting secure digital transformation, this Personal Data Protection Policy has been adopted to regulate the collection, processing, storage, use, and disclosure of personal data. The Policy aims to safeguard the rights of data subjects while enhancing trust in the University's educational, administrative, and research services.

October 6 University affirms that this Policy is fully aligned with the provisions of Egyptian Personal Data Protection Law No. 151 of 2020 and its Executive Regulations. It is also based on internationally recognized best practices in personal data protection and information security, thereby supporting the achievement of the Sustainable Development Goals (SDGs) and reinforcing the principles of transparency, accountability, and risk management.

Second: Purpose

This Policy aims to:

1. Protect the personal data of all University stakeholders.
2. Ensure compliance with the provisions of Egyptian Personal Data Protection Law No. 151 of 2020.
3. Preserve the confidentiality, integrity, and availability of personal data.
4. Regulate the collection, processing, use, storage, and disclosure of personal data.
5. Enhance the confidence of students, employees, faculty members, and partners in the University's digital systems.
6. Support secure digital transformation and institutional governance.
7. Minimize the risks of data leakage, unauthorized disclosure, or misuse.

Third: Scope of Application

This Policy applies to all personal data collected or processed by October 6 University and covers all affiliated entities, including:

- Faculties
- Institutes

- General administrative departments
- Specialized centers and units
- University hospitals and teaching clinics
- Research centers
- Libraries
- Information Technology Centers
- E-learning systems
- Student Information Systems (SIS)
- Human Resources Information Systems (HRIS)
- All faculty members, staff, students, trainees, visitors, contractors, and any individuals whose personal data are processed by the University.

Fourth: Definitions

For the purposes of this Policy, the following terms shall have the meanings assigned to them:

Personal Data

Any information relating to an identified or identifiable natural person, whether directly or indirectly.

Sensitive Personal Data

Personal data relating to health, genetic, biometric, financial, or any other categories designated by law as sensitive.

Processing

Any operation performed on personal data, including collection, recording, organization, storage, use, analysis, modification, transfer, sharing, retrieval, deletion, or destruction.

Data Controller

The entity that determines the purposes and means of processing personal data.

Data Processor

Any natural or legal person that processes personal data on behalf of the Data Controller.

Data Subject

The natural person to whom the personal data relates.

Fifth: Fundamental Principles of Personal Data Protection

The University is committed to the following principles:

1. Lawfulness

All personal data processing activities shall be conducted in accordance with applicable laws and regulations.

2. Transparency

The University should clearly inform data subjects about the reasons for collecting their personal data and how such data will be used.

3. Purpose Limitation

Personal data shall be collected for specified, explicit, and legitimate purposes and shall not be processed for incompatible purposes except where permitted by law.

4. Data Minimization

Only the minimum amount of personal data necessary to achieve the intended purpose shall be collected and processed.

5. Accuracy

The University shall take reasonable steps to ensure that personal data are accurate, complete, and kept up to date.

6. Confidentiality

Personal data shall be protected against unauthorized access, disclosure, alteration, or misuse.

7. Accountability

All University faculties, departments, centers, and units are responsible for complying with this Policy and documenting data protection practices within their respective areas.

Sixth: Collection of Personal Data

The University shall:

- Collect personal data through lawful and legitimate means.
- Collect only the minimum information necessary for the intended purpose.
- Clearly specify the purpose of data collection in advance.
- Inform data subjects about how their data will be used.
- Obtain consent whenever required under applicable laws.

Seventh: Use of Personal Data

Personal data may be processed for the following purposes:

- Managing educational and academic activities.
- Student admission and registration.
- Examination administration.
- Issuing academic certificates and transcripts.
- Providing student services.
- Human resource management.
- Administration of university hospitals and teaching clinics.
- Conducting scientific research in accordance with ethical standards.
- Preparing institutional statistics and reports.
- Complying with legal and regulatory obligations.

Personal data shall not be used for any other purpose unless authorized by law or with the consent of the data subject, where applicable.

Eighth: Sharing Personal Data with Third Parties

Personal data may only be disclosed to third parties under the following circumstances:

- With the consent of the data subject.
- To comply with legal obligations.
- Under officially approved cooperation agreements.

- To satisfy requests from competent regulatory authorities.
- For scientific research purposes after anonymization or de-identification whenever feasible.

All recipients of personal data must maintain confidentiality and use the data solely for the purposes for which they were disclosed.

Ninth: Information Security

The University shall implement appropriate technical and organizational measures to safeguard personal data, including:

- Encryption of sensitive personal data.
- Firewalls and network security controls.
- Anti-malware and endpoint protection systems.
- Access control and user privilege management.
- Multi-Factor Authentication (MFA).
- Regular data backup procedures.
- Business continuity and disaster recovery measures.
- Continuous monitoring to detect cybersecurity threats and unauthorized access.
- Regular updating and patching of software and information systems.

Tenth: Rights of Data Subjects

The University recognizes and protects the rights of data subjects as provided by applicable laws, including the right to:

- Be informed about how their personal data are processed.
- Access their personal data.
- Request correction of inaccurate or incomplete data.
- Update their personal information.
- Request deletion of personal data were permitted by law.
- Object to certain types of data processing in accordance with legal provisions.

Requests shall be handled in accordance with the University's approved procedures and applicable legal requirements.

Eleventh: Data Retention and Secure Disposal

The University shall:

- Retain personal data only for the period necessary to fulfill the purposes for which they were collected or as required by applicable laws and regulations.
- Periodically review retained data to ensure continued necessity.
- Securely dispose of paper and electronic records after the retention period using methods that prevent recovery or unauthorized access.

Twelfth: Data Breach Management

In the event of unauthorized access, disclosure, loss, or compromise of personal data, the University shall:

1. Immediately report the incident to the designated University authority.
2. Contain the incident and minimize its impact.
3. Investigate the root causes of the incident.
4. Implement corrective and preventive measures.
5. Document the incident and all actions taken.
6. Notify the competent authorities where required by applicable law.

Thirteenth: Training and Awareness

The University shall implement regular awareness and training programs covering:

- Personal data protection.
- Cybersecurity awareness.
- Secure use of digital systems.
- Prevention of phishing and social engineering attacks.
- Password security and authentication best practices.

- Proper handling of sensitive personal data.
- Responsibilities of faculty members, staff, and students regarding data protection.

Training materials should be reviewed and updated regularly to reflect technological developments and legislative changes.

Fourteenth: Review and Update

This Policy shall be reviewed at least once every three years, or whenever necessary due to:

- The issuance of new laws or regulations.
- Changes to University information systems.
- Internal or external audit findings.
- Emerging cybersecurity risks or threats.
- Institutional accreditation requirements or digital transformation initiatives.

Any amendments shall be approved by the University's competent authority before implementation.

Fifteenth: Responsibilities

All University faculties, departments, centers, and administrative units are responsible for implementing this Policy. Every member of the University community is responsible for protecting the personal data they handle and complying with the approved procedures and controls.

The relevant University departments—including the Information Technology Department, Digital Transformation Office, Legal Affairs Department, and Quality Assurance Center—shall oversee the implementation of this Policy, provide technical and awareness support, monitor compliance, and submit periodic reports to the University Administration.

Sixteenth: Final Provisions

This Policy shall enter into force on the date of its approval and shall be binding upon all University employees, faculty members, students, contractors, and all parties dealing with the University.

Any violation of this Policy shall constitute a breach of University regulations and may result in appropriate administrative or legal action in accordance with applicable laws and University regulations.

October 6 University is committed to providing the resources necessary for the effective implementation of this Policy and to continuously improving its data protection practices in order to strengthen personal data security, support secure digital transformation, reinforce the principles of governance and transparency, and ensure full compliance with national legislation and international best practices.

President of October 6 University

Prof. Mamdouh Ghorab

October [illegible]
Established [illegible]
Presidential Decree
No. 243/1996