ECU
EGYPTIAN CHINESE UNIVERSITY
الجامعة المصرية الصينية
EDUCATION NEW ERA

Data Protection Policy

Data Protection Policy

Statement of Policy

ECU is committed to protecting the privacy, confidentiality, integrity, and security of personal data relating to students, academic staff, administrative employees, researchers, alumni, partners, and visitors.

The University shall process personal data lawfully, fairly, transparently, and securely in accordance with:

- Egyptian Personal Data Protection Law No. 151 of 2020
- Applicable Egyptian higher education regulations
- International best practices for information security and privacy protection
- Ethical standards governing academic and administrative operations

Purpose

This Policy aims to:

- Protect personal and sensitive data handled by ECU
- Define responsibilities for data collection, storage, processing, transfer, and disposal
- Ensure compliance with Egyptian data protection legislation
- Promote transparency and trust in university operations
- Reduce risks related to unauthorized access, misuse, disclosure, or cyber threats

Scope

This Policy applies to:

- All ECU colleges, departments, centers, units, and administrative offices
- All university employees, faculty members, students, contractors, consultants, and third-party service providers
- All physical and electronic records containing personal data
- All university systems, websites, platforms, applications, and databases

Definitions

Personal Data

Any information relating to an identifiable natural person including:

- Name

- National ID/passport number
- Student or employee ID
- Phone number
- Email address
- Academic records
- Financial information
- IP address
- Biometric or health-related data

Sensitive Personal Data

Data relating to:

- Health conditions
- Biometrics
- Religious beliefs
- Financial status
- Criminal records
- Any information requiring enhanced protection under law

Data Subject

Any identifiable individual whose data is processed by ECU.

Processing

Any operation involving personal data including collection, recording, storage, use, sharing, transfer, or deletion.

Principles of Data Protection

ECU ensures that personal data is:

- Processed lawfully and fairly
- Collected for legitimate academic and administrative purposes
- Limited to necessary information only
- Accurate and regularly updated
- Stored securely and confidentially
- Retained only for necessary periods
- Protected against unauthorized access, alteration, disclosure, or destruction

Lawful Basis for Processing

ECU process personal data where:

- The data subject has provided consent
- Processing is necessary for academic administration

- Processing is required by law or governmental authorities
- Processing is necessary for employment obligations
- Processing is required to protect vital interests
- Processing supports legitimate educational and research purposes

Rights of Data Subjects

Individuals whose data is processed by ECU have the right to:

- Access their personal data
- Request correction of inaccurate information
- Withdraw consent where applicable
- Request restriction of processing
- Request deletion where legally permissible
- Be informed of how their data is used
- File complaints regarding misuse of personal data

Data Collection and Usage

ECU collects personal data for purposes including:

- Student admission and registration
- Academic records management
- Human resources administration
- Research activities
- Financial and tuition management
- Library and LMS services
- Campus security and safety
- University communications and events
- Accreditation and quality assurance processes

Personal data is not be used for unrelated purposes without lawful justification.

Data Security Measures

ECU implements appropriate technical and organizational safeguards including:

- Secure servers and encrypted databases
- Access control mechanisms
- Password protection and multi-factor authentication
- Regular cybersecurity monitoring
- Backup and disaster recovery procedures
- Staff awareness and training programs
- Secure disposal of records and storage media

Data Sharing and Disclosure

ECU may share personal data only:

- With authorized governmental authorities
- With accredited educational or research partners
- With service providers under confidentiality agreements
- When legally required
- With explicit consent from the data subject

Unauthorized disclosure of personal data is strictly prohibited.

International Data Transfers

Any transfer of personal data outside Egypt shall comply with applicable Egyptian laws and ensure adequate protection standards.

Data Breach Management

Any suspected or confirmed personal data breach must be reported immediately to the designated university authority.

ECU:

- Investigate incidents promptly
- Mitigate risks and damages
- Notify relevant authorities where required
- Take corrective and preventive actions

Data Retention

The University retains personal data only for as long as necessary to fulfill the purposes for which it was collected or as required by applicable legal and regulatory obligations.

The University is committed to:

- Data retention periods shall be reviewed periodically and adjusted, where necessary, to reflect the nature of the data and the purposes of processing.
- Periodically reviewing retained data to ensure its continued necessity.
- Securely deleting, destroying, or anonymizing personal data once the applicable retention period has expired or when the data is no longer required.
- Retaining academic, financial, and administrative records in accordance with applicable higher education laws, regulations, and requirements of competent regulatory authorities.

- Implementing secure disposal procedures for both physical and electronic records to prevent unauthorized recovery, access, or misuse.

Record Category	Retention Period
Student academic transcripts and degree records	Permanent
Student admission applications (unsuccessful applicants)	2 years
Student disciplinary records	5 years after graduation or separation
Student attendance records	5 years
Student financial aid records	7 years
Student medical records	7 years after last attendance
Employee personnel files	7 years after employment ends
Payroll and tax records	7 years
Recruitment records (unsuccessful applicants)	2 years
Research project records	5–10 years after project completion
Research ethics approvals	10 years
Research data containing personal information	5–10 years or as required by funding agreements
Financial and accounting records	7 years
Procurement and contract records	7 years after contract termination
CCTV recordings	30–90 days unless required for investigations
Visitor logs	1 year
IT system access logs	1–3 years
Email records (general business communications)	3–7 years
Library borrowing records	Until return of materials plus 1 year
Alumni contact information	Until consent is withdrawn or no longer required
Accreditation and quality assurance records	10 years or permanent for key institutional reports

Data Protection Officer (DPO)

The University appoints a Data Protection Officer (DPO) or designates a competent authority responsible for overseeing compliance with personal data protection requirements throughout the University.

The responsibilities of the Data Protection Officer include:

- Monitoring compliance with the Egyptian Personal Data Protection Law No. 151 of 2020 and related internal policies and procedures.
- Providing guidance and support to university departments on matters related to data protection and privacy.
- Supervising data processing activities and assessing associated risks.
- Receiving and addressing inquiries, requests, and complaints related to personal data protection.

- Coordinating with relevant regulatory and supervisory authorities when required.
- Overseeing awareness, education, and training programs concerning data protection and information security.
- Monitoring the reporting and management of personal data breaches and ensuring appropriate corrective actions are taken.
- Preparing periodic reports for senior management regarding compliance status and data protection risks.

Individuals may contact the Data Protection Officer through the official communication channels designated by the University regarding any inquiries, requests, or complaints related to personal data.

Responsibilities

University Administration

- Ensure institutional compliance
- Allocate resources for data protection measures

Employees and Faculty

- Handle data responsibly and confidentially
- Follow university security procedures

Students

- Use university systems responsibly
- Protect login credentials and personal information

IT Department

- Maintain cybersecurity and data protection infrastructure
- Monitor systems and respond to threats

Policy Violations

Violation of this Policy results in:

- Disciplinary action
- Suspension of access privileges
- Administrative penalties
- Legal action where applicable

Policy Review and Updates

This Policy shall be reviewed at least annually and updated whenever new legislation, regulatory requirements, or operational needs necessitate revision.