



OFFICE OF THE PRINCIPAL DIGITIZATION AND DATA PROTECTION OFFICER

General Privacy Notice – ICT Department

1. Data Controller

Mount Kenya University (MKU) is the Data Controller responsible for the collection and processing of personal data in connection with the University's Information and Communication Technology (ICT) services, systems, infrastructure and operations.

MKU is committed to protecting personal data and processing it in accordance with the **Data Protection Act, 2019**, applicable regulations, and the University's data protection policies and procedures.

2. Personal Data We May Collect

The ICT Department may collect and process the following categories of personal data, where necessary:

- Full name;
- Staff/student identification number;
- National ID or passport details, where required;
- Telephone number and email address;
- Department, School, Directorate, Campus or ODeL Centre;
- Job title, role or student status;
- Usernames, account and system identification details;
- Institutional email and other account information;
- System access and authentication information;
- Device, computer and equipment allocation details;
- IP addresses, MAC addresses and other network identifiers;
- Login, access, authentication and system activity logs;
- Information relating to ICT support requests, incidents and service tickets;
- Software, applications, licences and system access assigned to an individual;
- Internet, network and information-system usage information, where lawfully collected;
- CCTV or access-control information where ICT systems support such services;
- Electronic communications and technical metadata where necessary for ICT administration, security or troubleshooting;

- Information relating to cybersecurity incidents, investigations and response activities;
- Digital signatures and other electronic identifiers;
- Photographs or other identification information where required for ICT-enabled services; and
- Any other information reasonably necessary for the provision, administration, security and support of University ICT services.

3. Purposes of Processing

MKU may process personal data for purposes including:

- Creating and managing user accounts and access privileges;
- Providing ICT services, systems, applications and technical support;
- Managing institutional email and communication systems;
- Administering computer, network, server, cloud and other ICT infrastructure;
- Managing devices, ICT equipment and software licenses;
- Authenticating users and controlling access to University systems;
- Maintaining system availability, performance and reliability;
- Monitoring and protecting University networks, systems and information assets;
- Detecting, preventing and responding to cybersecurity threats and incidents;
- Investigating suspected unauthorized access, misuse, fraud or other security incidents;
- Maintaining system, network and security logs;
- Supporting business continuity, disaster recovery and system restoration;
- Managing ICT-related requests, complaints and service incidents;
- Conducting system audits, vulnerability assessments and security reviews;
- Implementing data protection and information security controls;
- Supporting digitization and electronic records management;
- Managing integrations between University systems and authorized third-party platforms;
- Meeting contractual, legal, regulatory and institutional requirements;
- Supporting ICT planning, reporting, service improvement and resource management; and
- Performing other legitimate University functions related to ICT administration and information security.

4. Lawful Basis for Processing

MKU will process personal data on one or more applicable lawful bases, including:

- Compliance with a legal or regulatory obligation;
- Performance of a contract or provision of University services;
- Performance of a task carried out in the public interest or in accordance with applicable institutional authority;

- Protection of information systems, University assets and the safety and security of individuals;
- Legitimate institutional interests, where applicable; and
- Consent, where consent is required by law.

5. ICT Systems, Logs and Monitoring

University ICT systems may automatically generate and retain technical information such as login records, IP addresses, device identifiers, system access records, timestamps, network activity and security logs.

Where necessary and lawful, ICT systems may also be monitored to:

- Maintain system security and availability;
- Detect and prevent cyber threats;
- Investigate security incidents;
- Troubleshoot technical problems;
- Protect University information and ICT resources;
- Ensure compliance with applicable policies and legal requirements; and
- Support audits and investigations.

Monitoring will be conducted in accordance with applicable law, University policies and authorized ICT and information security procedures.

6. Sharing and Disclosure of Personal Data

Personal data may be accessed or disclosed, where necessary and lawful, to:

- Authorized MKU ICT personnel and relevant University offices;
- System owners, data owners and authorized process owners;
- University management and authorized administrators;
- Authorized third-party technology and ICT service providers acting as data processors;
- Cloud service providers and software/application providers where authorized;
- Internet, telecommunications and other infrastructure service providers;
- Government agencies and regulatory authorities where legally required;
- Law enforcement agencies, courts or other authorized investigative bodies;
- Auditors, cybersecurity professionals and other authorized professional advisers; and
- Other authorized parties where disclosure is required or permitted by law.

MKU will take appropriate measures to ensure that third parties processing personal data on behalf of the University are subject to appropriate contractual, technical and organizational safeguards.

7. International or Third-Party Processing

Where University ICT services involve cloud platforms, hosted applications or other service providers that process personal data outside Kenya, MKU will implement appropriate safeguards and ensure that such processing is undertaken in accordance with applicable data protection requirements.

8. Data Security and Confidentiality

MKU implements appropriate technical and organizational measures to protect personal data and University information systems against:

- Unauthorized access;
- Unauthorized disclosure;
- Loss or destruction;
- Accidental or unlawful alteration;
- Cybersecurity threats;
- Malware and other malicious activities; and
- Other forms of unlawful or unauthorized processing.

Such measures may include access controls, authentication mechanisms, encryption, backups, monitoring, logging, vulnerability management, cybersecurity controls and staff awareness and training.

Access to personal data and ICT systems is restricted to authorized persons based on their roles and legitimate business requirements.

9. Data Retention

Personal data contained in ICT systems, logs, service records, user accounts and related documentation will be retained only for as long as necessary to fulfil the purposes for which it was collected, meet operational and security requirements, resolve disputes, investigate incidents and comply with applicable legal, regulatory, audit and institutional record-retention requirements.

When personal data is no longer required, it will be securely deleted, disposed of or anonymized in accordance with applicable University procedures.

10. Data Subject Rights

Subject to applicable legal conditions and limitations, data subjects may have rights to:

- Be informed about the processing of their personal data;
- Access their personal data;
- Request correction of inaccurate or incomplete personal data;
- Request deletion of personal data where applicable;
- Object to certain processing activities;
- Request restriction of processing in applicable circumstances;
- Withdraw consent where processing is based on consent; and
- Lodge a complaint with the relevant data protection authority.

Requests relating to personal data should be directed to the University Data Protection Officer.

11. Accuracy of Information

Individuals providing personal data to the ICT Department are expected to provide accurate, complete and up-to-date information and to notify the University where relevant information changes.

12. Contact the Data Protection Officer

For enquiries concerning this Privacy Notice, personal data processing, or to exercise applicable data protection rights, please contact:

Data Protection Officer

Mount Kenya University

Email: dataprotection@mku.ac.ke

Telephone: 0709 153 165

SHORT PRIVACY NOTICE FOR ICT FORMS AND SYSTEMS

PRIVACY NOTICE:

Mount Kenya University collects and processes the personal data provided through this form/system for purposes related to the provision and administration of ICT services, user account and access management, technical support, network and system administration, cybersecurity, system monitoring, incident management, audit, accountability and compliance with applicable legal and institutional requirements. ICT systems may generate technical and security logs, including information relating to system access, devices and network activity, where necessary and lawful. Your information will be accessed only by authorized persons and may be disclosed to authorized third parties where necessary or required by law. MKU will apply appropriate technical and organizational safeguards and retain the information in accordance with applicable legal and institutional requirements. You have rights regarding your personal data under the Data Protection Act, 2019. For enquiries or to exercise your data protection rights, contact the University Data Protection Officer at **dataprotection@mku.ac.ke** or **0709 153 165**.

Privacy Notice Version: 1.0

Effective Date: _____

Review Date: _____