



OFFICE OF THE PRINCIPAL DIGITIZATION AND DATA PROTECTION OFFICER

General Privacy Notice – Security Department

Data Controller: Mount Kenya University (MKU)

Mount Kenya University (MKU) is committed to protecting the privacy and security of personal data collected and processed through its Security Department and related security operations. This Privacy Notice explains how MKU collects, uses, stores, protects and discloses personal data for purposes of maintaining safety, security and the protection of persons, property and University facilities.

Personal data will be processed in accordance with the **Data Protection Act, 2019** and applicable data protection requirements.

1. Personal Data We May Collect

Depending on the security activity or process, MKU may collect and process personal data including:

- Full name;
- Staff or student identification/registration number;
- National identification/passport details, where applicable;
- Contact details, where necessary;
- Department, School, Directorate, Campus or organizational unit;
- Visitor information;
- Vehicle registration number and vehicle details;
- Date and time of entry and exit;
- Identification documents presented for verification;
- Access-control and identification records;
- Photographs and identification images;
- CCTV/video surveillance footage;
- Incident, accident and security reports;
- Information relating to lost and found property;
- Security clearance and access authorization information;
- Details of persons involved in security investigations;

- Signatures and acknowledgements; and
- Other information reasonably necessary for legitimate security purposes.

Where security operations involve sensitive personal data, MKU will process such information in accordance with applicable legal requirements and appropriate safeguards.

2. Purposes of Processing

Personal data collected through Security Department processes may be processed for purposes including:

- Protecting the safety and security of students, staff, visitors and other persons;
- Controlling and monitoring access to University premises and facilities;
- Verifying identity and authorization;
- Monitoring entry and exit from university premises;
- Managing visitor and vehicle access;
- Protecting University property, equipment, assets and information;
- CCTV and other security surveillance;
- Prevention, detection and investigation of theft, fraud, unauthorized access, misconduct and other security incidents;
- Recording and investigating accidents, incidents and security events;
- Supporting emergency response and management;
- Conducting security assessments and investigations;
- Supporting disciplinary or administrative investigations where applicable;
- Responding to lawful requests from government agencies, law-enforcement agencies and other authorized authorities;
- Maintaining security and access records;
- Supporting audit, accountability and institutional governance; and
- Other legitimate purposes necessary to protect the University community and its assets.

3. Lawful Basis for Processing

MKU processes personal data collected through Security Department activities on lawful grounds provided under applicable data protection law, including where processing is necessary to:

- Comply with a legal or regulatory obligation;
- Protect the safety and security of individuals;
- Protect University property, facilities and other legitimate institutional interests;
- Perform a task carried out in the public interest or in the exercise of official authority, where applicable;

- Pursue legitimate institutional interests, where applicable and where the rights and interests of the data subject are appropriately considered; or
- Process information with the data subject's consent where consent is required.

4. CCTV and Video Surveillance

MKU may operate CCTV and other video surveillance systems at selected University premises for legitimate security and safety purposes.

CCTV footage may be used to:

- Monitor and protect University premises;
- Detect and investigate security incidents;
- Support investigations involving theft, damage, unauthorized access or other incidents;
- Assist emergency response; and
- Provide evidence to authorized investigators, regulators, law-enforcement agencies or courts where lawfully required.

CCTV footage will be accessed only by authorized persons and retained in accordance with applicable legal and institutional requirements.

5. Access and Disclosure of Personal Data

Security-related personal data may be accessed by authorized MKU security personnel and other University officers where access is necessary for legitimate security, safety, administrative or investigative purposes.

Where required or permitted by law, relevant information may also be disclosed to:

- Law-enforcement agencies;
- Government ministries, departments and agencies;
- Courts and other lawful authorities;
- Emergency response agencies;
- Auditors or authorized investigators;
- Authorized security service providers and data processors; and
- Other authorized parties where disclosure is necessary for a legitimate security purpose or required by law.

MKU will take appropriate measures to ensure that personal data is disclosed only to authorized recipients and for legitimate purposes.

6. Data Security and Confidentiality

MKU implements appropriate technical and organizational measures to protect security-related personal data against unauthorized access, loss, misuse, alteration, disclosure, destruction or other unlawful processing.

Access to security records, CCTV footage, incident reports and other security information will be restricted to authorized personnel based on their roles and responsibilities.

7. Data Retention

Security-related personal data will be retained only for as long as necessary to fulfil the purposes for which it was collected and in accordance with applicable legal, regulatory, security, audit and institutional records-retention requirements.

CCTV footage, visitor registers, access records, incident reports and other security records may have different retention periods depending on their purpose and applicable requirements.

When personal data is no longer required, it will be securely disposed of, deleted, anonymized or otherwise handled in accordance with MKU's approved records-retention procedures and applicable law.

8. Rights of Data Subjects

Subject to applicable legal conditions and limitations, data subjects have rights in relation to their personal data, including the right to:

- Be informed about the collection and use of their personal data;
- Access their personal data;
- Request correction of inaccurate or misleading personal data;
- Object to certain forms of processing;
- Request restriction of processing where applicable;
- Request deletion of personal data where legally applicable; and
- Exercise other rights provided under applicable data protection law.

Some requests may be subject to legal, security, investigative, regulatory or records-retention requirements.

9. Accuracy of Information

Persons providing information to the Security Department are responsible for providing accurate, complete and up-to-date information.

Where information changes or an error is identified, the relevant Security Department office should be notified promptly so that appropriate corrective action can be taken.

10. Data Protection Queries and Requests

For questions concerning the processing of personal data, or to exercise applicable data protection rights, please contact:

Data Protection Officer

Mount Kenya University (MKU)

Email: dataprotection@mku.ac.ke

Telephone: 0709 153 165

Privacy Notice for Security Forms and Registers

The following abbreviated notice may be placed directly on MKU Security Department forms, visitor registers, vehicle registers and other security records:

PRIVACY NOTICE:

Mount Kenya University collects and processes personal data provided in this form/register for purposes related to security, access control, visitor and vehicle management, protection of persons and property, incident management, investigations, CCTV surveillance, accountability and compliance with applicable legal and institutional requirements. 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 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: 5th Jan 2025

Review Date: