KABARAK UNIVERSITY

STAFF/FACULTY PRIVACY NOTICE

1. Introduction

Kabarak University, also known as the **Data Controller** (registration number: 971-3513-7C00 with the Office of the Data Protection Commissioner), is dedicated to protecting your data. We ensure that all personal information we handle is processed in full compliance with Kenyan data protection laws.

This notice outlines how we use **personally identifiable information (PII)** for individuals who are, or have been, associated with Kabarak University. This includes all potential, current, or former employees, consultants, contractors, volunteers, interns, and academic visitors. If you are in one of these groups, you are considered a **"data subject"** under this policy. As a staff member, you are also legally and contractually obligated to protect the personal information of others, such as students and research participants.

We encourage you to read this notice carefully, along with any other privacy notices we may issue when collecting your personal data.

Please note that this notice is for informational purposes only and is not a part of any employment or service contract you may have with the university.

2. What is Personal Data

Personal data refers to any information about you from which you can be identified from that information alone or taken together with other information. It does not include data where your identity has been removed and where you can no longer be identified (anonymized data). It is important that the personal data that we hold about you is accurate and current. Please keep us informed if your personal data changes during your working relationship with us.

3. Who will process my personal information?

This notice details Kabarak University's procedures for holding and processing your personal data. If you are also employed by another organization while working for Kabarak University, that organization will have its own privacy statement explaining how they handle your personal information.

4. What personal information will we process?

The University requires to collect, maintain and use personal data relating to or about you. This may include:

a) **Personal details:** Your name, title, addresses, phone numbers, email, date of birth, gender, and marital status, along with details of your dependents, next of kin, and emergency contacts.

b) **Identification and payroll information:** National ID/Passport number, NHIF, NSSF, and KRA PIN numbers, bank account details, and tax details. This also covers your salary, leave, pension, and benefits information.

c) **Employment history:** Your start and end dates, job location, work history, titles, working duration, and training records.

d) **Recruitment and professional documentation:** Your CV, cover letter, references, professional certifications, professional license, and, if applicable, a passport and visa to confirm your right to work.

e) **Performance and conduct:** Information about your role, performance reviews, sickness records, and any disciplinary or grievance details.

f) **Security and systems data:** CCTV footage, biometric data (collected with your explicit consent and for specific, legally compliant purposes), and information about your use of our information communication systems.

g) **University facilities and interests:** Data regarding your use of academic and non-academic facilities, as well as a Register of Interests for relevant staff.

h) **Additional data:** Photographs, video clips, voice recordings and information from public sources, such as your publications, may also be included.

5. What constitutes "Sensitive Personal Data"?

The University will also process some information about you that is considered more sensitive and this is referred to as 'sensitive personal data' personal data as inscribed in the Data Protection Act 2019. When we process this type of information, we are required to apply additional protections. Sensitive personal data is defined as racial or ethnic social origin, beliefs, conscience, health status-including mental health and disability information, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex life and sexual orientation, genetic data and biometric data which is processed to uniquely identify a person.

6. What is the purpose of the processing under data protection law?

Based on the information you provided, the purpose of processing your data falls under one or more of these **legal bases**:

- **Contractual Necessity:** This means your data is processed to fulfill the terms of a contract or agreement you have with the university. For example, using your personal details to enroll you in a course, maintain your employment with us.

- **Legal Obligation:** The university is legally required to process your data to comply with a law or regulation. This could include reporting information to a government body and agencies.

- **Legitimate Interests:** The university has a valid reason to process your data for its own operations, as long as your fundamental rights and interests aren't harmed. An example could be using data for internal administrative purposes to improve services.

- **Vital Interests:** This is a more critical legal basis, used when processing is necessary to protect your life or the life of another person.

- **Public Interest/Official Purposes:** The university may process data for tasks that are considered to be in the public interest or for its official functions as a public serving institution.

These conditions ensure that the university can only use your personal information when there is a clear, legal justification for doing so.

7. Reasons for Processing your Personal Data

Examples of the reasons or purposes the University will process your personal data, including where appropriate sensitive personal data include the following:

7.1 To assess your suitability for a particular job, role or task (including any relevant right to work checks) and deciding whether or not to employ or engage you.
7.2 Determining the terms on which you work for the University.
7.3 Checking that you are legally entitled to work in Kenya.
7.4 Paying you, and, where applicable, making deductions as required by law.
7.5 Liaising with your pension provider.
7.6 Administering the contract that we have entered into with you, including where relevant, its termination.
7.7 Business management and planning including accounting and auditing.
7.8 Conducting performance reviews, managing performance and determining performance requirements.
7.9 Making decisions about salary reviews and benefits.
7.10 Assessing qualifications for a particular job, role or task, including decisions about promotions.
7.11 Carrying out a disciplinary or grievance or Dignity at Work investigation or procedure in relation to you or someone else.
7.12 Making decisions about your continued employment or engagement.
7.13 Assessing education, training and development requirements.
7.14 Monitoring compliance by you and the University with our policies and contractual obligations.
7.15 Monitoring and protecting the security (including the University's network, information and electronic communications systems) of the University, of you, our staff, students or other third parties.
7.16 Monitoring and protecting the health and safety of you, our staff, students or other third parties.
7.17 Ascertaining your fitness to work and managing sickness absence.
7.18 To support you in implementing any health-related adjustments to allow you to carry out a particular role or task.
7.19 Dealing with legal disputes involving you or other employees, workers and contractors, including accidents at work.
7.20 Preventing fraud.
7.21 Paying trade union subscriptions.
7.22 Conducting data analytics studies, for example, to review and better understand employee retention rates.

7.23 To provide a reference upon request from a third party.

7.24 To comply with employment law, immigration law, contract law, health and safety law and other laws which affect the University. Where relevant, to monitor, evaluate and support your research and commercialization activity.

7.25 To operate security (including CCTV), governance, audit and quality assurance arrangements, including producing a staff identity card which also involves the collection and storage of a digital photograph.

7.26 To deliver facilities (e.g., IT, libraries), services (e.g., accommodation) and staff benefits to you, and where appropriate to monitor your use of those facilities in accordance with the University policies (e.g., on the acceptable use of IT)

7.27 To communicate effectively with you by post, email and phone, in the form of newsletters and bulletins with the intention of keeping you informed about important developments and events relevant to your role at the University. Where appropriate you will be given an opportunity to opt out of receiving these communications.

7.28 To invite you to participate in staff surveys and compile statistics and conduct research for internal and statutory reporting purposes.

7.29 If you are also a student at Kabarak University we may also use your staff data for student administration purposes.

7.30 To support your training, health, safety, welfare and religious requirements.

7.31 To fulfil and monitor our responsibilities under equalities, immigration and public safety legislation and to monitor the effectiveness of the Equality and Diversity strategy.

7.32 To enable us to contact others in the event of an emergency (we will assume that you have checked with the individuals before you supply their contact details to us).

8. How we will use your Sensitive personal data?

We only process your **sensitive personal data** when there is a legal justification to do so.

In some situations, we will ask for your **explicit consent**. If we do, we will explain exactly what data we need and why, so you can make an informed decision. You can withdraw your consent at any time, and giving consent is never a condition of your contract with us.

However, your consent is **not always be the only legal basis required**. We can also process sensitive data when it's necessary to:

- Meet our legal obligations.
- Handle data you have already made public.
- Protect your vital interests or those of another person, especially if you or they are unable to give consent.
- Handle legal claims.
- Assess your working capacity on health grounds.

How We Use Your Sensitive Personal Data

Specifically, we use this type of data for the following purposes:

- **Equal Opportunity Monitoring:** We use your race, nationality, ethnic origin, religious beliefs, and sexual orientation to monitor and report on equal opportunities.
- **Legal Compliance:** We use information about absences (due to sickness or family leave) to comply with employment laws.

- **Health and Safety:** We use information about your physical or mental health and disability status to ensure your safety at work, assess your fitness to work, provide necessary adjustments, manage sickness, and administer benefits.
- **Membership:** We use your membership information to manage subscriptions and comply with legal obligations related to membership benefits.

9. How we will process criminal convictions and offences information

9.1. The university will only process information about your criminal convictions and offenses when it's legally permissible and relevant to your role.

9.2. **Legal Basis for Processing**
Primarily, this data will be processed when it is necessary for the university to carry out its legal obligations.

9.3. In less common situations, the university may also use this information for:

a. **Legal Claims**: To establish, exercise, or defend legal claims.

b. **Vital Interests:** To protect your interests or the interests of another person, particularly if you are unable to give consent.

c. **Publicly Available Data:** If you have already made the information public yourself.

10. What if I fail to provide personal data?

If you fail to provide personal data that the university reasonably requests, it may hinder the university's ability to fulfill its obligations to you or comply with its own legal requirements. For example, if you don't provide necessary information, the university may not be able to administer your contract, manage your rights, or meet its legal duties.

11. Who will my personal information be shared with?

Your personal data is shared as permitted or required by law, on a considered and confidential basis, with a range of external organizations, including the following:

11.1. Prospective and research funders or sponsors.
11.2. The external service providers of the University, including benefits, rewards, health insurance providers, health providers, IT service providers.
11.3. Medical Insurance provider;
11.4. The University's professional adviser(s);
11.5. Relevant Government Departments, and Higher Education agencies (e.g., Commission for University Education, Ministry of Education, Higher Education Loans Board).
11.6. Relevant professional or statutory regulatory bodies (e.g., NHIF/SHA, NSSF, KRA, NEA).
11.7. If you are a member of a pension scheme, we will share information with the administrators of that scheme.
11.8. The relevant professional bodies subscribed to;

11.9. The police and other law enforcement agencies;
11.10. Auditors;
11.11. Subsidiary companies of the University where necessary;
11.12. Companies or organizations providing specific services to, or on behalf of, the University;
11.13. We will provide references about you to external enquirers or organizations where you have requested or indicated that we should do so;
11.14. We will include your basic contact details in our internal online directory, though you can control how much information is accessible internally. You may also choose to make your details available externally; you can choose at any time to change these settings via the self-service interface;
11.15. Information about senior staff and certain other staff (e.g. appointments or committee memberships) is published by the University.

On occasion, the above types of sharing may involve the transfer of your personal data outside Kenya (e.g., to report to an overseas research funder, scholarship or exchange programme). Such transfers usually are necessary in order to meet our contractual obligations with you, and are carried out with appropriate safeguards in place to ensure the confidentiality and security of your personal information.

In addition to the above, we may publish or disclose any personal information about you to external enquirers or organizations if you have requested it or consented to it, or if it is in your vital interests to do so (e.g., in an emergency situation).

12. How does the University protect personal information?

The university is committed to protecting your personal information. To do so, they have implemented a range of security measures.

12.1 Security Measures in Place

a) **Technical and Organizational Protections:** The university has established appropriate security measures to prevent your data from being lost, used, or accessed without authorization.
b) **Restricted Access:** Access to your personal information is limited to university employees, agents, contractors, and other third parties who have a legitimate business need to view it.
c) **Confidentiality:** All personnel who process your data are required to follow the university's instructions and are bound by a duty of confidentiality.
d) **Secure Storage:** Your personal information is stored securely in both paper format and in specialized databases, such as the ERP.

12.2 Handling Data Breaches

In the event of a suspected data security breach, the university has procedures in place to manage the incident. They will also inform you and the relevant regulatory body, such as the Office of the Data Protection Commissioner, as they are legally required to do so.

13. What are my rights in connection with my personal information?

Under certain circumstances, by law, you have the right to:

13.1. Request access to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.

13.2. Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected. If you believe any of your personal data/ information we hold is incorrect, you should amend it via the Staff Portal. If you cannot make the required change via the Staff Portal, please contact the Human Resources department.

13.3. Request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing.

13.4. Object to processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.

13.5. Request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

13.6. Request the transfer of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the Data Management Officer.

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

If you would like to exercise any of these rights, you should contact the University Data Management Officer by email: dpo@kabarak.ac.ke.

14. How long is my information kept?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of your personal information are available in our Records Retention Schedule.

In some circumstances, we may anonymize your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the University we will retain and securely destroy your personal information in accordance with our data retention policy and applicable laws and regulations.

15. Who can I contact if I have any queries?

If you have any questions about how your personal information is used by the University as a whole, or wish to exercise any of your rights, please consult the University's Data Management Officer: dpo@kabarak.ac.ke

16. Complaints

If you wish to raise a complaint about how we have handled your personal data, you can contact the University Data Management Officer who will investigate the matter.

Our Data Management Officer can be contacted at dpo@kabarak.ac.ke, or by writing to Data Management Office, P.O. Private Bag - 20157, Kabarak, Nakuru.

If you are not satisfied with our response or believe we are not processing your personal data in accordance with the law, you can complain to the Data Commissioners Office (ODPC) https://www.odpc.go.ke)

17. Updates to this privacy notice

We may update this privacy notice from time to time in response to changing legal, technical or business developments. When we update our privacy notice, we will take appropriate measures to inform you, consistent with the significance of the changes we make.