



KABARAK UNIVERSITY

DATA PRIVACY STATEMENT

Version 2.0 Dated 31st May 2025

1. Policy Statement

Kabarak University and all its campuses are dedicated to protecting your fundamental right to privacy. As a registered Data Controller with the Office of the Data Protection Commissioner (ID: 971-3513-7C00), we handle personal data in accordance with the Kenya Data Protection Act of 2019 and other relevant Kenyan laws. We respect the privacy of the personal information and data we collect from you through various channels.

This Privacy Statement applies to the personal data Kabarak University collects and handles to support teaching, learning, community outreach, administration and other university-related activities. For the purpose of this statement, "**personal data**" refers to any information that relates to an identified or identifiable natural person.

2. Scope

This privacy statement notice applies to all users of Kabarak University services and platforms, and is subject to the Data Protection Act, 2019 and related laws in Kenya.

3. Responsibilities

This privacy statement is monitored and updated by the Data Management Officer in collaboration with the University Webmaster and the Corporate Communications and Marketing Department.

4. Who we are.

Kabarak University of P.O PRIVATE BAG – 20157, KABARAK is a data handler registered as a data controller with respect to the personally identifiable data it handles and processes in connection with the services provided under the relevant engagement with its customers, staff and stakeholders.

5. What Personal Data Do We Collect About You?

As a Data Controller, Kabarak University collects personal data directly from the Data Subject or indirectly through government agencies, service providers, and other third parties. We may collect the following personal information, which may vary depending on your relationship with the university (e.g., student, staff, visitor, or applicant etc.).

Types of Information	Examples
Identification and Contact Information	Name, address (and proof of address), other contact details (e.g., email, telephone, emergency contact details), gender, marital status, date and

	place of birth, nationality, next of kin, parent/guardian details (for minors or dependents).
Government-Generated Information	National ID Number, Tax PIN, Passport Details, NHIF & NSSF Details, driver's license, immigration or visa status (for international students or staff).
Employment and Educational Information	Employment history, educational background (including institutions attended, qualifications, certifications, transcripts), professional memberships, references, disciplinary records, performance evaluations, academic records (e.g., grades, attendance, course enrolment), research outputs, and publications.
Financial Information	Bank account details (e.g., account number, bank name, payment history), financial aid or scholarship details, tuition payment records, loan information, billing information, and sponsorship details.
Health-Related Information	Health data: current or former medical conditions, health status, relevant personal habits (e.g., smoking, alcohol consumption), prescription information, medical history, disability status, vaccination records, and health insurance details.
Audio-Visual Information	Photographs (e.g., passport photo, ID photos, event captures), videos, audios, CCTV footage (installed at strategic locations to provide a safe and secure work and learning environment across all campuses as part of our commitment to security and crime prevention), voice recordings (e.g., for virtual learning or interviews).
Online Activity Information	IP address, pages viewed, actions on university websites or platforms (e.g., learning management systems, library portals), login credentials, cookies, and tracking data for analytics or security purposes.
Biometric Data	Fingerprints, or other biometric identifiers used for secure access to university facilities, systems, or services (e.g., catering payments, library access, attendance tracking, or examination verification).
Demographic and Socioeconomic Information	Ethnicity, religion, socioeconomic background (for financial aid purposes), and language proficiency.
Behavioural and Disciplinary Information	Student/ Staff conduct records, disciplinary actions, academic integrity violations, attendance patterns, and participation in extracurricular activities or university events.
Application and Admission Information	Application forms, entrance exam results, recommendation letters, personal statements, admission status, and enrolment details.
Communication and Correspondence Information	Emails, letters, text messages, chat logs, or other communications with university staff, faculty, or systems (e.g., support tickets, inquiries, or feedback).
Survey and Feedback Information	Responses to university surveys, feedback forms, course evaluations, or satisfaction surveys.

Event and Participation Information	Records of participation in university events, workshops, seminars, sports, clubs, or societies, including registration details and attendance logs.
Location and Travel Information	Travel history (for international students or staff), or accommodation details (e.g., on-campus housing assignments).
Emergency and Safety Information	Emergency contact details, medical emergency protocols, evacuation drill participation, or incident reports related to safety on campus.
Research and Academic Project Data	Data related to research activities, grant applications, intellectual property, or collaborative projects.
Alumni and Post-Graduation Information	Post-graduation contacts details, employment status, further studies, alumni association membership, and related details.

This is not an exhaustive list. Kabarak University may collect further personal data during our interactions with you, based on your role (e.g., prospective student, employee, or alumnus). All data collection adheres to applicable data protection laws and is used strictly for legitimate purposes, such as academic administration, campus security, or enhancing your university experience.

6. Where We Collect Your Personal Information

Kabarak University collects personal information to support our teaching, learning, community outreach, administrative, and operational activities. The purposes for which we use your personal information depend on your relationship with the university (e.g., student, employee, prospective student, parent/guardian, alumni, partner, visitor, or contractor) and the nature of our interactions, including the services we provide and the communications between us.

We collect personal data from various sources, including but not limited to:

- a) **Directly from Individuals and their Representatives:** Information provided by you or your family members (e.g., parents/guardians or emergency contacts) through application forms, enrolment forms, financial aid applications, employment forms, payment forms, or other university-related documentation.
- b) Data submitted via online portals, such as the student information system, staff intranet, or alumni registration platforms.
- c) Information shared during meetings, telephone conversations, email correspondence, or other direct communications with university staff, faculty, or departments.
- d) Responses to surveys, feedback forms, course evaluations, or event registration forms.
- e) **Third Parties and External Entities:** Educational institutions, such as high schools, colleges, or examination bodies (e.g., Kenya National Examinations Council), providing academic records, transcripts, or admission test results.
- f) Employers or referees, for employee recruitment or student internship/placement verification.
- g) Government agencies, such as the Kenya Revenue Authority (tax details), National Hospital Insurance Fund (NHIF), National Social Security Fund (NSSF), Higher Education Loans Board (HELB), or immigration authorities (for international students or staff).

- h) Service providers, such as financial institutions (for payment processing), health providers (for medical records or insurance).
- i) Professional bodies or certification agencies, for verifying qualifications or memberships.
- j) Law enforcement or regulatory bodies, in cases involving legal or disciplinary matters (e.g., police reports or court orders).
- k) Partners or sponsors, such as scholarship providers, research collaborators, or exchange program coordinators.
- l) **University Systems, Platforms and Technologies:** Our website (www.kabarak.ac.ke) including data collected via cookies, web forms, or analytics tools tracking user interactions (e.g., page visits or downloads).
- m) Software applications (apps) provided by the university, such as mobile apps for students, staff, or alumni to access services like course registration, library resources, or campus navigation.
- n) Learning management systems (e.g., Moodle or similar platforms), capturing data on course participation, assignments, or online assessments.
- o) Campus security systems, such as CCTV cameras, access control systems (e.g., biometric or card-based entry), or Wi-Fi networks logging device information.
- p) Email systems, chat platforms, or other communication tools used for university-related interactions.
- q) **Public and Social Media Sources:** Social media platforms (e.g., Twitter, Facebook, LinkedIn, Instagram) where you engage with the university's official accounts or public posts, including comments, messages, or shared content.
- r) Publicly available information, such as professional profiles (e.g., LinkedIn) or publications, used for recruitment, alumni engagement, or research purposes.
- s) **Events and On-Campus Activities:** Information collected during university events, such as open days, orientation, graduation ceremonies, workshops, or sports activities, through registration forms, attendance logs, or media capture (e.g., photographs or videos).
- t) Data from on-campus interactions, such as library usage, dining hall transactions, or participation in student organizations.
- u) **Other Sources:**
 - i) Alumni networks or associations, providing updates on post-graduation activities, contact details, or donations.
 - ii) Research activities, where participants provide data through surveys, interviews, or experiments (with appropriate consent).
 - iii) External auditors or accreditation bodies, sharing data during institutional reviews or quality assurance processes.

We ensure that personal data is collected lawfully, transparently, and only for specified purposes, such as academic administration, campus safety, service delivery, research, or enhancing your experience with the university. All data collection complies with applicable data protection regulations.

7. Use of Your Personal Data

Kabarak University uses your personal data to deliver academic excellence, support our operations, and enhance your experience as a member of our community. The purposes for which we use your personal data depend on your relationship with the university (e.g., student, employee, prospective student, parent/guardian, alumnus, partner, or visitor, or contractor) and the services we provide. We may use your personal data for the following purposes:

a) Identity Verification and Enrolment:

- i) Verifying your identity and eligibility for academic programs, employment, or other university services (e.g., confirming academic credentials, employment history, or financial aid eligibility).
- ii) Conducting background checks or due diligence for student admissions, staff recruitment, or scholarship awards, where applicable.

b) Academic and Educational Services:

- i) Administering teaching, learning, and assessment activities, including course registration, grading, examination management, and certification issuance of transcripts or degrees.
- ii) Supporting academic advising, research activities, and access to library resources, learning management systems, or online learning platforms.
- iii) Facilitating internships, exchange programs, placements, or industry partnerships to enhance your educational experience.

c) Communication:

- i) Communicating with students, employees, prospective students, parents/guardians, alumni, and other stakeholders via email, phone, text messages, or other channels for academic, administrative, or operational purposes (e.g., class schedules, fee reminders, or event invitations).
- ii) Responding to inquiries, feedback, or complaints submitted through our website, feedback forms, or other communication channels.

d) Employment and Human Resource Process Management:

- i) Processing applications, employment, onboarding, payroll, benefits, and performance evaluations for staff, faculty, and contractors.
- ii) Managing staff training, professional development, and compliance with employment regulations.

e) Teaching and Learning Service Improvement and Personalization:

- i) Enhancing university services, such as improving academic programs, campus facilities, or digital platforms, based on feedback and usage data.
- ii) Personalizing your experience, such as recommending courses, events, or resources tailored to your interests or academic needs, while ensuring appropriate safeguards for your personal data.

f) Campus Safety and Security:

- i) Ensuring a safe and secure environment through CCTV monitoring, access control systems (e.g., biometric or card-based entry), and incident reporting.
- ii) Managing emergency protocols, including contacting emergency contacts or coordinating with authorities when necessary.

g) Financial and Administrative Operations:

- i) Processing payments for tuition, accommodation, catering or other services, including managing financial aid, scholarships, or refunds.
- ii) Maintaining accurate records for accounting, billing, auditing, and budgeting purposes.

h) Compliance with Regulatory Requirements:

- i) Fulfilling obligations to regulatory bodies, such as the Commission for University Education (CUE), Office of the Data Protection Commissioner (ODPC), Kenya Revenue Authority (KRA), Higher Education Loans Board (HELB), and other relevant authorities, including submitting reports or responding to audits.
- ii) Complying with legal obligations, such as data protection laws, labour laws, or court orders.

i) Marketing and Engagement:

- i) Providing information about university programs, events, or services through communication channels like email, text messages, or social media, where you have provided explicit consent or opted in to receive such communications.
- ii) You may opt out of our marketing communications or use of your personal data/information for marketing purposes at any time by clicking “Unsubscribe” in the footer of emails or SMS messages or by contacting us directly as indicated below.
- iii) Engaging with alumni and stakeholders to promote university initiatives, fundraising campaigns, or alumni events.

j) Information Technology and System Management:

- i) Operating and securing IT systems, such as student portals, email services, and cloud-based platforms, to ensure reliable access to university resources.
- ii) Monitoring system usage to maintain information security and prevent unauthorized access or cyber threats.

k) Institutional Research and Analysis:

- i) Conducting institutional research to assess academic performance, student satisfaction, or operational efficiency, using anonymized or aggregated data where possible.

l) Event and Community Participation:

- i) Managing participation in university events, such as open days, graduation ceremonies, sports, or cultural activities, including registration, attendance tracking, and media capture (e.g., photos or videos, with consent where required).
- ii) Facilitating student organizations, clubs, or societies to foster community engagement.

We are committed to using your personal data lawfully, transparently, and only for the purposes outlined above, in accordance with this Privacy Statement and applicable data protection laws. Where required, we will obtain your consent or provide you with options to control how your data is used (e.g., opting out of marketing). Appropriate measures, such as data minimization and encryption, are implemented to protect your personal information.

8. Legal Justification for Our Use of Personal Data

The primary purpose for collecting and processing your personal data is to perform contractual and statutory tasks related to management of the teaching and learning service we provide. We will also process your data in connection with other tasks as required by law and statutory regulations. We commit to always identify and document without prejudice the lawful basis of processing your personal data for each specific purpose and put necessary security measures to ensure safeguarding of your personal data and the lawful purpose consented to always applies.

9. How We Store and Protect Your Data

We have put in place appropriate physical, legal, technical and organizational safeguards to protect the personal data we collect in connection with our services. Such measures include but are not limited to requiring confidentiality from employees and other persons authorize to handle personal data and implementing information technology security measures such as system rights, audit trails and firewalls.

You should be aware that the Internet is not a secure form of communication and sending and receiving information over the Internet carries with it risks including the risk of access and interference by unauthorized third parties. We do not accept responsibility or liability for the

confidentiality, security or integrity of your Personal Data in connection with its transmission over the Internet.

10. Disclosure of Personal Data.

Kabarak University is committed to keeping your personal data confidential and will only disclose it when necessary to fulfill the purposes for which it was collected, as required by law, or with your prior consent. Depending on your relationship with the university (e.g., student, employee, prospective student, parent/guardian, alumnus, partner, or visitor), we may share your personal data with relevant third parties to support our academic, administrative, and operational activities.

In addition to the disclosures outlined in the table below, we may share your personal data with service providers, contractors, or agents who perform activities on our behalf (e.g., IT service providers, payment processors, or campus security firms), subject to strict confidentiality agreements and compliance with applicable data protection laws, such as the Data Protection Act of Kenya (2019).

Purpose of Processing	Legal Grounds	Disclosure
Academic Administration Administering academic programs, including enrolment, course management, examinations, and certification.	<ul style="list-style-type: none"> - Performance of a contract (including student enrolment, staff employment). - Legitimate interests of the university (to deliver educational and academic services). - Compliance with a legal obligation (e.g., reporting to regulatory bodies). 	<ul style="list-style-type: none"> - Government agencies (i.e. Commission for University Education (CUE), Kenya National Examinations Council (KNEC)). - Accreditation bodies. - External examiners or academic partners. - Learning management system providers.
Student Support Services Providing financial aid, scholarships, counselling, or accommodation services.	<ul style="list-style-type: none"> - Performance of a contract (i.e. financial aid agreements). - Consent (i.e. for sharing health data with counsellors). - Legitimate interests (to support student welfare). 	<ul style="list-style-type: none"> - Scholarship sponsors or funding bodies (e.g., Higher Education Loans Board (HELB)). - Health service providers (e.g., university clinic or external medical professionals). - Hostel Accommodation
Employment and Human Resources Managing recruitment, payroll, benefits, and staff performance.	<ul style="list-style-type: none"> - Performance of a contract (e.g., employment contract). - Compliance with a legal obligation (e.g., tax or labour laws). - Legitimate interests (to manage workforce operations). 	<ul style="list-style-type: none"> - Government agencies (e.g., Kenya Revenue Authority (KRA), National Hospital Insurance Fund (NHIF), National Social Security Fund (NSSF)). - Payroll or benefits providers. - Recruitment agencies or referees.
Financial Transactions Processing tuition fees, refunds, or other payments.	<ul style="list-style-type: none"> - Performance of a contract (e.g., payment agreements). - Legitimate interests (to manage financial operations). 	<ul style="list-style-type: none"> - Financial Institutions (Banks and payment processors). - Financial aid or loan providers (e.g., HELB). - Auditors or accounting firms.
Campus Safety and Security Ensuring a safe campus environment through CCTV, access control, or incident reporting.	<ul style="list-style-type: none"> - Legitimate interests (to ensure safety and security). - Compliance with a legal obligation (e.g., reporting incidents to authorities). - Consent (e.g., for biometric data use). 	<ul style="list-style-type: none"> - Security service providers. - Law enforcement agencies (e.g., police, in case of incidents). - Emergency services (e.g., medical or fire response teams).
Regulatory Compliance Meeting legal or regulatory requirements, such as audits or reporting.	<ul style="list-style-type: none"> - Compliance with a legal obligation. - Legitimate interests (to ensure regulatory compliance). 	<ul style="list-style-type: none"> - Regulatory bodies (e.g., CUE, Office of the Data Protection Commissioner (ODPC)). - External auditors or accreditation agencies.

		- Government authorities (e.g., KRA, Ministry of Education).
Institutional Research and Analysis Conducting academic or institutional research, including surveys or studies.	- Legitimate interests (to improve academic programs or operations).	- Research collaborators or funding agencies. - Institutional review boards. - Data analytics providers (using anonymized data where possible).
Marketing and Engagement Promoting university programs, events, or alumni activities.	- Consent (e.g., for marketing communications). - Legitimate interests (to engage with stakeholders).	- Marketing service providers (e.g., email or SMS platforms). - Alumni associations. - University website and Social media platforms (with consent).
Event Management Organizing events such as open days, graduation, or workshops.	- Performance of a contract (e.g., event registration). - Legitimate interests (to facilitate community engagement). - Consent (e.g., for sharing photos or videos).	- Event organizers or vendors - Media outlets (for public events, with consent). - Photographers or videographers.
IT and System Operations Managing university systems, such as student portals, email, or Wi-Fi networks.	- Performance of a contract (e.g., access to systems). - Legitimate interests (to maintain secure IT systems and operations).	- IT service providers (e.g., cloud storage or cybersecurity firms). - Software vendors (e.g., ERP Support Vendor, for learning management systems etc.).
Legal or Disciplinary Matters Addressing legal claims, academic misconduct, or disciplinary issues.	- Legitimate interests (to resolve disputes or enforce policies). - Compliance with a legal obligation. - To establish, defend, or prosecute legal claims.	- Legal advisors or law firms. - Disciplinary committees. - Law enforcement or regulatory bodies (e.g., The police, ODPC).

Kabarak University will not disclose your personal data to third parties, such as service providers or partners, without your prior consent, unless it is necessary for a legitimate purpose, to perform a contract, or as required by law. All disclosures are made in compliance with applicable data protection regulations, and we ensure that third parties receiving your data are bound by confidentiality obligations and use the data only for the specified purpose.

11. Consent

To deliver our academic, administrative, and support services, Kabarak University may rely on your consent, where required by law, to process certain types of personal data such as photos, videos, health records, financial details, or biometric data. Your consent enables us to share this information with relevant third parties as necessary to fulfill the purposes outlined in this Privacy Statement.

By engaging with our services—such as enrolling as a student, applying for employment, accessing our website (www.kabarak.ac.ke), or participating in university activities—you acknowledge and agree to the terms of this Privacy Statement. If you are providing consent on behalf of another individual or entity (e.g., a sponsor/parent/guardian acting for a minor), you represent and warrant that you have the authority to do so.

In some cases, your consent to process personal data is necessary for us to provide the requested services, such as:

- Processing health or disability data to provide academic accommodations or medical support.
- Sharing academic records with accreditation bodies or partner institutions for certification or exchange programs.

- Using your photos, videos or contact details for marketing purposes about university programs or events (where you have opted-in).

Providing Data About Others: If you provide us with personal data about another person (e.g., emergency contact details or family information), you agree to inform them of how we will use their data, as described in this Privacy Statement, and to obtain their consent where required.

Withdrawing Consent: You may withdraw your consent to the processing of your personal data at any time by contacting us through the designated channels (e.g., email or the university's data protection office). However, please note that withdrawing consent may limit our ability to provide certain services, such as:

- Access to specific academic or support programs requiring sensitive data (e.g., financial aid or health accommodations).
- Participation in events or activities where data sharing is necessary (e.g., sharing details with event organizers).
- Continued enrolment or employment, if the data is essential for contractual or legal obligations (e.g., reporting to regulatory bodies like the Commission for University Education).

We will respect your decision to withdraw consent and take appropriate steps to cease processing the relevant data, subject to any legal or contractual requirements. For example, if you withdraw consent for sharing data with a third party (e.g., a scholarship provider), it may affect your eligibility for that service.

Kabarak University is committed to processing your personal data transparently and in compliance with applicable data protection laws, including the Data Protection Act of Kenya (2019). We will only seek your consent when necessary and ensure that any third parties receiving your data are bound by confidentiality obligations.

12. Transfer of Your Personal Data

Kabarak University may transfer your personal information for the purpose of effecting/implementing, administering, and securing any academic program or service that you have applied for or for other purpose set out in this privacy statement. We may disclose or transfer the personal data we collect to regulatory or supervisory authority, third-party contractors, subcontractors, and/or their subsidiaries and affiliates who provides support to Kabarak University in providing its services. These third-party providers may use their own third-party subcontractors that have access to personal data (sub-processors). It is our policy to use only third-party providers that are bound to maintain appropriate levels of security and confidentiality, to process personal information only as instructed by Kabarak University, and to follow those same obligations down to their sub-processors.

13. Cross-border Transmission of Your Personal Data

Your data is primarily stored in our data servers located within Kenya. Where we send your information outside the country, we will make sure that there is proof of adequate data protection safeguards in the recipient country or consent from you on transfer of your personal information.

Prior to transferring personal data outside the country where you are located, we shall ascertain that the transfer is based on the provided legal and regulatory standards.

Circumstances in which we may transfer your personal data outside are highlighted in the table below;

Legal Basis	Example
An adequacy decision having being made by the Office of the Data Commissioner	Where the Data Commissioner has published a list of countries which have appropriate data protection safeguards and we decide to store your data in that jurisdiction in furtherance to our legitimate interest.
Consent	When following your express consent, we transfer your personal data to another jurisdiction.

14. Retention of Personal Data

Personal Data is retained as long as necessary for the purpose for which it is collected and to meet legal, regulatory and operational requirements. Retention periods may differ depending on the nature of personal data collected. At the end of the retention period, anonymized data is kept for management information purposes. Kabarak University has also put in place Records retention policy in line with Data Protection law.

Kabarak University may also retain your contact information for the purposes of service engagement from time to time and may use your contact to send you notifications notifying you of our various programs, surveys, and university updates. You are responsible for the confidentiality of any password you have put in place to allow you to access certain services or platforms. Please note our staff will never request you to share your password.

15. Your Data Protection Rights

We will collect, process and store your personal data in accordance with your rights under the Data Protection Act and attendant Regulations. Under certain circumstances, you have the following rights in relation to your personal data:

DESCRIPTION OF RIGHT	APPLICABILITY
<i>Right to object to processing of personal data</i> – You have a right to object to the processing of their personal data. In implementation of this right, you shall use the form “Request for restriction or objection to the processing of personal data” provided in our website.	The right is not an absolute right and we can reject the request where we demonstrate that we have justifiable reasons for processing that would negate your interests e.g. when we are required by a government agency exercising their legal mandate to provide your personal data against your request not to avail the same or in our defense of a legal claim. We will always inform you when we have declined your request and provide the reasons. This right is however absolute when it relates to direct marketing.

Right to restrict processing of personal data

– You have the right to request the suspension of processing of your personal data in certain circumstances. In implementation of this right, you shall use the form “Request for restriction or objection to the processing of personal data” provided in our website

This right is not an absolute right and shall be available when

- You contest the accuracy of your personal data
- Your personal data has been unlawfully processed and you oppose the erasure and request restriction instead
- You no longer need your personal data but we require the same to be kept in order to establish, exercise or defend a legal claim
- You have objected to the processing, pending verification as to whether our use of your personal data is justifiable and overrides your interest.

Right to access personal data – You have the right to access your personal data and obtain information of how the said personal data is used and processed. In implementation of this right, you shall use the form “Request for access to personal data” provided in our website

You may access your personal data through our Self-Service Portals. Should you want to access your personal data in any other format, you may use the form subject to availing us available notice and other circumstances as shall be communicated by us to you.

Right to rectification of personal data– You have the right to request your personal data to be corrected in instances of inaccuracy or incompleteness. In implementation of this right, you shall use the form “Request for rectification” provided in our website.

The right is available always subject to the discretion accorded to us to decline with reasons

Right to data Portability – You have the right to receive your personal data in a structured, commonly used and machine-readable format, to transmit the said personal data obtained to another third party without any hindrance. In implementation of this right, you shall use the form “Request for Data Portability” provided in our website

This right is available always provided that it is technically feasible for us to provide the personal data in the required format.

Right to erasure – This right is sometimes referred to as “the right to be forgotten” and entitles you to request deletion or removal of your personal data from our records. In implementation of this right, you shall use the statutory form “Request for

Right of erasure does not apply if processing of your personal data is necessary for one of the following reasons.

- To exercise the right of freedom of expression and information

erasure of personal data “provided in our website	<ul style="list-style-type: none"> • To comply with a legal obligation e.g. our requirement to hold on to your personal data in the event of an ongoing investigation. • For the performance of a task carried out in the public interest or in the exercise of social authority • For archiving purposes in the public interest, scientific research, historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing. • For the establishment, exercise or defense of a legal claim.
<i>Right to withdraw consent to processing of personal data.</i>	This right only applies where personal data is processed based upon your consent.
<i>Rights relating to automated decision making and profiling</i> – You have a right not to be subjected to a decision based solely on our automated processing, including profiling, which legally and significantly affects you.	<p>This right is not applicable when a decision is:</p> <ul style="list-style-type: none"> • Authorized by a law to which we are subject and which lays down suitable measures to safeguard your rights, freedoms and legitimate interests • Based on your consent

In exercising your right as provided above, we may request specific information from you to help us confirm your identity. This is a security measure to ensure that Personal Data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

16. Enforcing Your Rights

If you wish to enforce any of your rights as highlighted above as provided under the Data Protection Act and Subsequent Regulations and sector specific guidelines, then please contact us on our details in clause 20 below. You may use the various forms made available by us and we will respond to your request without undue delay and within the stipulated timelines.

17. Complaints

If you feel we have not complied with your right to privacy and other provided rights regarding your personal data, you have a right to complain to us through the provided tool available on our website or you may pay us a visit and fill the complaint form and we shall purpose to resolve such a complain. You however have the right to contact the Office of the Data Commissioner.

18. Cookies

Cookies are small text files that our websites and apps store on your computer or device. When you visit our website and pages, we may use these technologies to recognize your device the next time you return.

We use cookies to make your online experience better. For example, they help you navigate our sites easily, remember your preferences, and generally improve how our websites function for you.

19. Changes to This Data Privacy Statement

Kabarak University reserves the right to change the provisions of this Privacy Statement at any time. Where the changes will have a fundamental impact on the nature of the processing of your data or your rights, we shall notify you in advance. We will let you know via email and/or a prominent notice on our website, prior to the change becoming effective and update the “effective date” at the top of this Privacy Statement.

Your use of the Website and applications following the posting of such revised Statement shall constitute your acceptance of any such changes. We encourage you to review our Privacy Statement whenever you visit the Website and application(s) to guarantee your understanding of how your information may be collected, processed and used.

20. Contact Information

If you have any queries relating to your personal data and/or this Privacy Statement, contact us through dpo@kabarak.ac.ke

Our address for purposes of data processing is;

Data Management Officer
Kabarak University
P.O. PRIVATE BAG – 20157 Kabarak, Kenya
dpo@kabarak.ac.ke | www.kabarak.ac.ke

Download the forms below to exercise your data subject rights access request:

ID	Form Title	Download
1.	Request for Access to Personal Data	Download
2.	Request for Data Portability	Download
3.	Request for Erasure of Personal Data	Download
4.	Request for Rectification of Personal Data	Download
5.	Request for Restriction or Objection to the Processing of Personal Data	Download
6.	Request for Restriction or Objection to the Processing of PII Data for Marketing Purposes	Download