STAFF PRIVACY NOTICE

1. Introduction

KCA University is registered as a Data Controller with the Office of the Data Protection Commissioner (ODPC) (Identification: 349-5820-E44E), and we are committed to ensuring that the data we process is handled in accordance with data protection law.

This notice provides information about the use of personal information while you are a current or former employee, worker, consultant, officer, contractor, volunteer, intern, casual worker, agency worker, apprentice, affiliated lecturer or academic visitor at KCA University. If you fall into one of these categories, then you are a "data subject" for the purposes of this notice. As a member of staff (or equivalent) you also have certain legal and contractual responsibilities to protect the personal information of other people (e.g. other employees, students, research participants) by handling it appropriately.

It is important that you read this notice, together with any other privacy notices we may provide on specific occasions when we are collecting or processing personal data about you. By way of example only, this could be when you engage with University services such as the Staff Counselling Service or Occupational Health.

This notice does not form part of any contract of employment or other contract to provide services.

2. 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 explains how KCA University will hold and process your personal information. If you are employed simultaneously by another body, subsequent to your KCA university employment, that organization will provide you with its own statement setting out how it will use, share and disclose your personal information.

4. What personal information will you process?

The University needs to collect, maintain and use personal data relating to or about you. This includes:

4.1. Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses

4.2. Date of birth

4.3. Gender

4.4. Marital status and dependents

4.5. Next of kin and emergency contact information

4.6. National ID number

4.7. NHIF number

4.8. NSSF number

4.9. Bank account details, payroll records and tax status information

4.10. Salary, annual leave, pension and benefits information

4.11. Employment Start date

4.12. Location of employment or workplace

4.13. Copy of driving license

4.14. Copy of passport and where relevant visa and right to work documentation

4.15. Recruitment information (including copies of right to work documentation, details of your experience, education and training, references and other information included in a CV or cover letter or as part of the application process)

4.16. Employment records (including job titles, work history, working hours, training records and professional memberships)

4.17. Salary, benefits and compensation history

4.18. Details about your role(s) in the University, including any information relating to your undertaking of such role(s) (for example copies of performance information including Performance and Development Reviews, sickness records)

4.19. Disciplinary and grievance information

4.20. CCTV footage and other information obtained through electronic means such as swipe-card records

4.21. Biometric data in acceptable purposes for collecting and subject to explicit consent from individuals, when necessary for processing employment contracts, in compliance with legal obligations, vital interests, and legitimate interests pursued by the employer while ensuring data protection and individual rights.

4.22. Information about your use of our information and communications systems.

4.23. Photographs

4.24. Information about your use of the academic and non-academic facilities and services that we offer

4.25. A Register of Interests, covering all academic staff and any support staff, who have relevant interests to disclose. Where relevant, we may supplement these records with personal data from the public domain (e.g. your publications) or other sources.

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 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?

We will only use your personal information when the law allows us to do so by providing us with a legal basis or valid condition. Most commonly, we will use your personal information in the following circumstances:

6.1. Where we need to perform the contract we have entered into with you.

6.2. Where we need to comply with a legal obligation.

6.3. Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

6.4. Where we need to protect your vital interests (or someone else's interests).

6.5. Where it is needed in the public interest or for official purposes.

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 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 photographs.

7.26. To deliver facilities (e.g. IT, libraries), services (e.g. accommodation, childcare) and staff benefits to you, and where appropriate to monitor your use of those facilities in accordance with 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 KCA 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 will only process sensitive personal data in certain situations in accordance with the law. For example, we can do so if we have your explicit consent and, in some circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do, we will provide you with full details for the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent, which you can withdraw at any time. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.
We do not need your consent to process sensitive personal data when we are processing it for the following purposes as these satisfy another legal condition:

8.1. where we need to carry out our legal obligations

8.2. where you have made the data public

8.3. where it is necessary to protect your vital interests or those of another person and where you/they are physically or legally incapable of giving consent

8.4. where processing is necessary for the establishment, exercise or defense of legal claims

8.5. where it is needed to assess your working capacity on health grounds

In particular, we will use your sensitive personal data in the following ways:

8.6. your race, national or ethnic origin, religious, philosophical or moral beliefs or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

8.7. information relating to leaves of absence, which may include sickness absence or family related leaves to comply with employment and other laws.

8.8. your information about your physical health or mental health or disability status to ensure your health and safety in the workplace and to assess your fitness to work, provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits

8.9. your information about trade union membership to pay any subscriptions and to comply with our legal obligations in respect of trade union members

9. How we will process criminal convictions and offences information

9.1. We will only process information relating to criminal convictions if it is appropriate given the nature of the role and where it is in accordance with the law. This will usually be where such processing is necessary to carry out our legal obligations.

9.2. Less commonly, we may use information relating to criminal convictions where it is necessary for the establishment, exercise or defense of legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

10. What if I fail to provide personal data?

We require you to provide us with any information we reasonably ask to achieve one or more of the purposes described above, for example to enable us to administer your contract or to comply with our legal obligations. If you fail to provide certain information when requested, this will hinder our ability to administer your rights and obligations relating to your relationship with the University or we may be prevented from complying with our legal obligations.

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 actual research funders or sponsors

11.2. The external service providers of the University, including benefits, rewards, health insurance providers, occupational health, IT service providers and pension providers.

11.3. Insurance providers

11.4. The University's professional advisers

11.5. Relevant Government Departments, and Higher Education bodies (e.g. Commission for University Education, and Higher Education Loans Board).

11.6. Any relevant professional or statutory regulatory bodies (e.g. ICPAK, NHIF, NSSF, KRA).

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 trade unions

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). 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 takes the security of your data seriously. We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorized way, altered or disclosed.

In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator (e.g. Office of the Data Protection Commissioner) of a suspected breach where we are legally required to do so. Your personal information is created, stored and transmitted securely both in paper format and in bespoke databases, such as the HR information system.

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 University personal information 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 Protection 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 Protection Officer by email: dpo@kcau.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 Protection Officer: dpo@kcau.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 Protection Officer who will investigate the matter.

Our Data Protection Officer can be contacted at dpo@kcau.ac.ke, by calling +254 710888022, or by writing to Data Protection Office, P.O. Box56808-00200, Nairobi, Thika Road, Ruaraka.

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.

Published on:	29th August 2023
Last Updated On:	29th August 2024
Next Review Date:	29th August 2025
Version Number:	2.0