MACHAKOS UNIVERSITY

DATA PROTECTION POLICY

JUNE, 2020

APPROVAL

Policy Title: Data Protection Policy

Policy Contact: Deputy Vice Chancellor (Research, Innovation and Linkages)

Approval Authority: The University Council

Category: Division of Research, Innovation and Linkages

Reference No.:.....

Effective date:.....

Approved by the University council:

Sign: ..... Date: 30/7/2020.....

PROF. LUCY W. IRUNGU, Ph.D.
VICE-CHANCELLOR & SECRETARY TO THE COUNCIL

Sign: ..... Date: Aug 4th 2020.

PROF. GIDEON HANJARI, Ph.D.
CHAIRMAN MACHAKOS UNIVERSITY COUNCIL

FOREWORD

In its daily operations, Machakos University' brings various actors and stakeholders, who bring and seek information. This information, broadly seen as data is key in informing decisions. Such data helps us to pursue our mission, which is to Provide scholarly education through Training, Research and Innovation for Industrial and socio-economic transformation of our communities and therefore must be protected and managed.

This Machakos University Data Protection Policy is anchored on Kenya Data protection legislations including the Data protection Act, 2019 and it sets out how the University will always protect data, including that generated through research and any such channel or medium as may be deemed necessary from time to time and case by case. As the University grows and embrace technology, information has increasingly become a critical resource that has to be managed carefully.

The Policy leverages the University in complying with data protection regulations All sharing of personal data with third parties will be subject to the appropriate controls as laid out in data protection legislation including but not limited to Kenya Data Protection Act, UK Data Protection Act, EU General Data Protection Regulations and any country specific regulations and protocols as may be deemed necessary.

In fulfilling its role in national development as envisaged by the national policy, legal and strategy documents as well as institutional strategy, the University purposes to entrench data Protection policy with the aim of protecting both the university's and personal data. This policy therefore provides a framework for the management of Data at Machakos University. The Policy is founded on our Strategic Plan 2019-2024.

The management commits itself to the implementation of this policy and will subject it to periodic views to ensure its relevance in line with the changing circumstances and changing needs of our university and our country.

PROF. LUCY IRUNGU, Ph.D.
VICE CHANCELLOR
&
PROFESSOR OF ENTOMOLOGY

DEFINITION OF TERMS AND CONCEPTS

Anonymization: The removal of personal identifiers from personal data so that the data subject is no longer identifiable.

Consent: Any manifestation of express, unequivocal, free, specific and informed indication of the data subject's wishes by a statement or by a clear affirmative action, signifying agreement to the processing of personal data relating to the data subject.

Data: Information which — (a) is processed by means of equipment operating automatically in response to instructions given for that purpose; (b) is recorded with intention that it should be processed by means of such equipment; (c) is recorded as part of a relevant filing system; (d) where it does not fall under paragraphs (a) (b) or (c), forms part of accessible record; or (e) is recorded information which is held by a public entity and does not fall within any of paragraphs (a) to (d).

Data protection legislation: Applicable laws and regulations relating to processing of personal data and privacy, including where applicable the guidance and codes of practice

Data Asset Registers: Catalogues of the information the University holds and processes, where it is stored, how it moves and who has access.

Data Commissioner's office: the independent regulatory office in charge of upholding information rights in the interest of the public.

Data protection officer: The University's responsible officer for data protection compliance.

Data Subject: A natural person whose personal data is processed by Machakos University or by an appointed data processor.

Data Controller: The entity that determines the purposes, conditions and means of processing of personal data.

Information Asset Owners: Heads of respective divisions. Are responsible for ensuring that specific information assets are handled and managed appropriately.

Information Compliance Unit: The department responsible to ensure that the University adheres to external rules and internal controls.

Personal data: Any information relating to an identified or identifiable natural person;

Personal data breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;

Processing: Any operation or sets of operations which is performed on personal data or on sets of personal data whether or not by automated means, such as (a) collection, recording, organization, structuring; (b) storage, adaptation or alteration; (c) retrieval, consultation or use; (d) disclosure by transmission, dissemination, or otherwise making available; or (e) alignment or combination, restriction, erasure or destruction.

Subject Access Request form: A form used to collect personal information to effectively and compliantly carry out our everyday functions and services to comply with the requirements of the law and/or regulations.

University's Privacy Impact Assessment process: A process which assists the university in identifying and managing privacy risks arising from new methods of collecting or handling personal information.

Table of Contents

1. 0. INTRODUCTION

This Policy is anchored on Kenya Data protection legislation including the Data protection Act, 2019 and it sets out how Machakos University protects data, including that generated through research, academic, administration and any such channel or medium as may be deemed from time to time and case by case. As the University grows and embrace technology, information has increasingly become a critical resource that has to be managed carefully. Generally, much of University's information consists of personal data relating to individuals, data generated through research and that shared for general knowledge and strategic partnerships.

Machakos University like other universities across the Globe experiences technological growth that has impacted the way data is generated, processed, stored and distributed. The University acknowledges the importance of accessing information and safeguarding it as articulated in the Kenya National ICT Policy as well as ICT Policy of Machakos University. As a result, the transformative developments in computing are presenting major concerns for privacy in the way information is processed.

The aim of the policy is to protect data in order to guard against misuse and to eliminate the unwarranted invasion of privacy. The fundamental principles of the policy have been largely informed by global practices and the need to bridge the gaps that exist in contextualizing privacy and data protection in technological environment in Machakos University.

The Policy has been prepared with specific reference to:

1. Machakos University ICT Policy, 2019
2. Kenya National ICT Policy, 2019
3. Constitution of Kenya, 2010
4. Kenya Data Protection Act, 2019
5. UK Data Protection Act, 2018(16),
6. EU General Data Protection Regulations and the data protection act 2018

2. 0. PURPOSE

The purpose of Machakos University Data Protection Policy is two-fold: 1) Protection of all personal information and 2) Protection of the rights and freedoms of individuals with respect to the processing of their personal and general information in research, academic and administration activities.

3. 0. OBJECTIVES OF MACHAKOS UNIVERSITY DATA PROTECTION POLICY

The Principal objectives of the Data Protection Policy are to:

1) Ensure Privacy and Data Protection practices at Machakos University and facilitate statutory and regulatory compliance, and enhance effective application;

2) Comply with the international good practice and ensure consistency in practices and procedures in developing and administering the Privacy and Data Protection laws;

3) Ensure effective protection and management of Personal Data by identifying, assessing, monitoring and mitigating privacy risks in programs and activities involving the collection, retention, use, disclosure and disposal of Personal Data;

4. 0 SCOPE

This policy sets out requirements for the protection of Personal Data in manual, electronic or any other emerging forms. The policy shall be the overarching guiding policy in relation to matters of Privacy and Data Protection. It applies to all entities in Machakos University that undertake processing of data belonging to natural persons.

The university processes personal information for a variety of reasons which it defines within its Privacy Notices, that include:

1) Administration of the student application process;
2) Academic, research, publication and innovation administration;
3) Managing human Resources processes, such as applications, performance management, training and development;
4) Administration of financial aspects of an individual's relationship with the university;
5) Management of use of facilities and participation in events;
6) Enabling effective communication with staff and students;
7) Operation of security, disciplinary, compliant and quality assurance processes and arrangements;

8) Support of Health, Safety and Welfare requirements;
9) Production of Statistics and research for internal and statutory reporting purposes;
10) Fundraising and Marketing.

5.0. PRINCIPLES FOR DATA PROTECTION

To comply with the policy, information must be collected and used fairly, stored securely and not disclosed to any other person unlawfully. The principles applied in the Policy are based on the global best practices in data protection.

5.1 Fairness and lawfulness and Transparency

5.1.1. Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

5.1.2 The processing of Personal Data must happen in a lawful way and have a legal or legitimate basis.

5.1.3 Personal data will be considered to have been obtained fairly if the data subject is informed of the name of the data controller and the purpose(s) for processing the personal data or any further information which is necessary, having regard to the specific circumstances in which the data is or is to be processed, to enable processing in respect of the data subject to be fair.

5.1.4 Data controller should be transparent regarding the processing of personal data and inform the data subject in an open and transparent manner. Personal data should only be processed if and only if there is a legitimate purpose for the processing of that personal data. A Data controller should practice transparency so that the data subjects will be sufficiently informed regarding the processing of their personal data. When processing personal data, the individual rights of data subject must be protected.

5.2 Purpose Limitation

5.2.1 Personal Data shall be collected for specified, explicit, and legitimate purpose and not further processed in a manner that is incompatible with those purposes.

5.2.2 Personal data must be processed only for the purpose that was defined before the data was collected.

5.2.3 Further processing for archiving purposes in the public interest, scientific interest or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purpose. Subsequent changes to the purpose are only possible to a limited extent and require legitimate basis.

5.3 Data Minimization

5.3.1. Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purpose for which the data will be processed.

5.3.2. Before processing personal data, a data controller must determine whether and to what extent the processing of personal data is necessary in order to achieve the purpose for which the data was required.

5.3.3. Personal data may not be collected in advance and stored for potential future purposes unless required or permitted by law.

5.3.4. Privacy and security should be built and integrated in from the onset in all data management systems that collect and process personal data. Such systems should have privacy incorporated by design or default.

5.4 Storage Limitation

5.4.1 Period for keeping Personal data shall take into account the University's' needs to process the data, as well as any legal obligations to keep the data for a fixed period of time.

5.4.2 There may be an indication of interests that merit protection or historical significance of this data in individual cases. If so, the data must remain on file until the interests that merit protection have been clarified legally, or the archive has evaluated the data to determine whether it must be retained for historical purposes subject to adequate protection against access or use for unauthorized purpose.

5.5 Accuracy

5.5.1 Personal data on file must be correct, complete, and be kept up to date.

5.5.2 Suitable steps must be taken by a data controller to ensure that inaccurate or incomplete data is deleted, corrected, supplemented or updated.

5.6 Confidentiality and Integrity

5.6.1 Personal data must be collected and processed securely to retain confidentiality and integrity in consistency, accuracy, and trustworthiness over its entire life cycle.

5.6.2 Steps must be taken to ensure that data cannot be altered by unauthorized entities or people.

5.6.3 Security of personal data shall be preserved by establishing suitable organizational and technical measures to prevent unauthorized access, illegal processing or distribution, as well as accidental loss, modification or destruction.

5.7 Accountability

All Data Controllers shall be responsible for personal data protection, and be able to demonstrate compliance to the principles on Data Protection.

6.0 DATA SUBJECT RIGHTS

The University will comply with all data subject rights, as appropriate in relation to the processing it undertakes as follows:

6.1 There may be limitations on data rights of data subject when required by the law or when there are competing rights and therefore would require an assessment based on the facts and circumstances. A data subject (an individual to whom personal data relates) has the following rights:

6.1.1 Right to access to personal information;

6.1.2 Right to information as to whether personal data is being processed;

6.1.3 The right to rectification if the information held is inaccurate or incomplete or requires to be updated;

6.1.4 The right to restrict processing of their personal data;

6.1.5 The right to object decisions solely based on automated processing circumstances such as automated processing, publication/ processing of sensitive personal data profiling which produces legal effects or significantly affects data subject;

6.1.6 The right to complain (as would be appropriate to the controller, processor or regulator).

7. The information Compliance Unit will perform periodic audits to ensure compliance with this policy and to ensure that the notification of the Information Commissioner is kept up to date and appropriate accountability can be demonstrated.

9. 0. PROCEDURES

9.1 INFORMATION ASSET OWNERS

1) Each area of the university that processes personal Data will fall under a head division, as Information Asset owner;

2) Information Asset owner manages an information or data asset and, in consultation with the Vice Chancellor, may make decisions about how that information is managed;

3) Information Asset Owners will work with the information Compliance Unit to disseminate guidance and information relating to data protection and good information handling practices, as well as managing breach reporting within their area and maintaining the appropriate registers to demonstrate accountability in relation to data protection.

9.2 RECORD OF PROCESSING

Information Asset Owners will be responsible for recording and processing data assets within the university's data register(s) and for maintaining this register.

9.3 PRIVACY IMPACT ASSESSMENTS

All major data processing activities, especially new processing of personal data or adaptations of existing methods of processing, are risk assessed using the university's Privacy Impact Assessment process to ensure that the proposed processing complies with the requirement of data protection.

9.4. TRANSPARENCY OF PROCESSING

Wherever personal data is collected for a new purpose, the information Asset Owner responsible for that data will ensure a Privacy Notice is created with data subjects. This Privacy Notice will include:

1. Name of data controller and contact details
2. Contact details of the University Data Protection Officer
3. Purposes of Processing the data
4. Legal basis of processing
5. Transfers outside the University and Kenya
6. Length of time for which data will be retained
7. Data subject rights in relation to the data
8. Recipients of the data
9. Statutory or contractual requirements to provide the data
10. Any automated decision-making including profiling
11. Right to complain to the Data Commissioner's office (DCO) if data is not processed in accordance with data protection principles.

Information Asset Owners should use guidance and templates made available by the Information Compliance Unit to create Privacy notices unless otherwise justifies by the circumstances.

9.5. SUBJECT ACCESS REQUESTS

Data protection Legislation gives data subjects the right to access any personal information held about them by Machakos University.

Any person can exercise this right by submitting a Subject Access Request form, available from the information Compliance Unit. Any formal subject access request must be responded to within the 30 calendar days, or appropriate additional timescale as laid down by data protection legislation, and must be notified to the information Compliance unit as soon as they are received.

9.6. DATA SHARING

All sharing of personal data with third parties will be subject to the appropriate controls as laid out in data protection legislation including but not limited to Kenya Data Protection Act, UK Data Protection Act, EU General Data Protection Regulations and country specific regulations and protocols.

Repeated or ongoing data sharing arrangements must be covered by an appropriate data sharing or processor agreement.

10.0 USE OF PERSONAL DATA WITHIN RESEARCH

1) Where research involves the processing of personal data, the Chief or Principal investigator will be considered to be relevant Information Asset Owner of the data.

2) All requirements of this policy relating to the processing of personal data should be adhered to alongside the University's research good practice requirements including but limited to Intellectual Property Policy, Research Policy, Anti-Plagiarism Policy, Open Access Policy and any such applicable University Policy as may be deemed appropriate from time to time.

3) Use of personal data for research will be subject to the appropriate safeguards as specified within the data protection legislation, in particular, personal data should be limited to the minimum amount of data which is reasonably required to achieve the desired academic objectives. Wherever possible, personal information should be anonymized or pseudonymized so that the data subjects cannot be identified.

4) Students should only obtain or use personal information relating to third parties for approved research or other legitimate university-related purposes with the knowledge and express consent of an appropriate information Asset Owner or member of staff who is responsible for their supervision.

11.0 GOVERNMENT REQUIREMENTS

This policy is communicated to all staff as part of the university induction process and there are no exceptions. Data protection legislation (Data Protection Act 2019) requires that all processing of personal data within the university be subject to an appropriate policy.

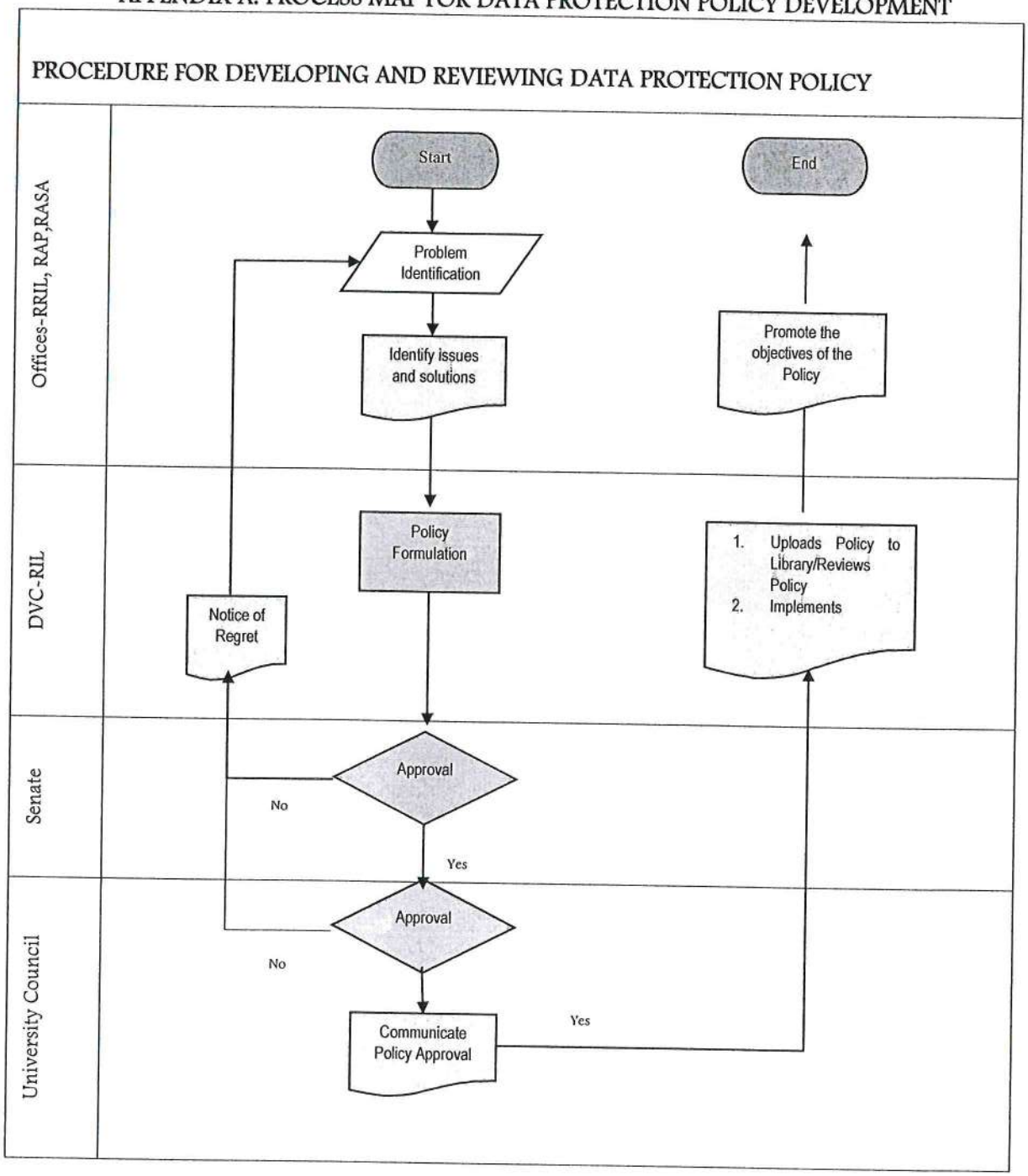
12. POLICY REVIEW

This policy will be reviewed after every three years from effective date or as needs arise.

13. EFFECTIVE DATE

This Policy shall take effect from the date of approval by the University Council.

APPENDIX A: PROCESS MAP FOR DATA PROTECTION POLICY DEVELOPMENT



APPENDIX A: PROCESS MAP FOR DATA PROTECTION POLICY IMPLEMENTATION