KENYA VETERINARY ASSOCIATION (KVA)

DATA PROTECTION POLICY AND PROCEDURES

DOCUMENT CONTROL

Field	Details
Document title	KVA Data Protection Policy and Procedures
Document owner	KVA Secretariat
Approving authority	National Executive Council (NEC)
Version	1.0
Status	Final, Approved and Adopted
Effective date	September 17, 2026
Applies to	KVA staff, NEC members, BEC Members, KVA members, consultants, interns, volunteers, contractors, service providers, partners, programme beneficiaries, research participants and other data subjects whose personal data KVA processes.
Review cycle	Every three years from latest effective date, or earlier following legal, technological or operational change, a significant data incident, or NEC direction.

VERSION CONTROL

Version	Date	Summary of changes	Approved by
1.0	17/09/2026	Initial policy for approval	NEC

RELATED KVA POLICIES AND PROCEDURES

- Safeguarding Policy and Procedures
- Health, Safety and Wellbeing Policy and Procedures
- GEDI commitments and guidance
- Human resource and staff conduct procedures
- Digital Compliance Guidelines

TABLE OF CONTENTS

DOCUMENT CONTROL 2
VERSION CONTROL 2
RELATED KVA POLICIES AND PROCEDURES 2
TABLE OF CONTENTS 3
1. POLICY STATEMENT 4
2. SCOPE AND OBJECTIVES 4
3. LEGAL AND REGULATORY FRAMEWORK 4
4. KEY DEFINITIONS 5
5. DATA PROTECTION PRINCIPLES 5
6. GOVERNANCE AND RESPONSIBILITIES 5
6.1 National Executive Council (NEC) 5
6.2 Chief Executive Officer (CEO) 5
6.3 Data Protection Officer / Designated Data Protection Focal Person 6
6.4 Administrative officers 6
6.5 All Personnel 6
7. DATA INVENTORY, PURPOSE AND LAWFUL PROCESSING 6
8. COLLECTION, PRIVACY NOTICES AND DATA MINIMISATION 6
9. SENSITIVE DATA, CHILDREN AND VULNERABLE DATA SUBJECTS 6
10. RESEARCH, SURVEYS, PROGRAMME MONITORING AND BENEFICIARY DATA 7
POLICY INTERACTION AND REFERRAL 7
11. PHOTOGRAPHS, VIDEO, AUDIO, STORIES AND COMMUNICATIONS 7
12. DATA QUALITY, ACCESS AND SECURITY 8
13. SHARING, PROCESSORS, PARTNERS AND INTERNATIONAL TRANSFERS 8
14. DATA RETENTION AND SECURE DISPOSAL 8
15. DATA SUBJECT RIGHTS AND REQUESTS 8
16. DATA PROTECTION IMPACT ASSESSMENTS AND PRIVACY BY DESIGN 9
17. PERSONAL DATA BREACH MANAGEMENT 9
18. REGISTRATION, TRAINING, MONITORING AND COMPLIANCE 9
19. COMPLAINTS AND ESCALATION 10
20. RECORD KEEPING AND POLICY REVIEW 10
21. APPROVAL AND AUTHORISATION 10
ANNEX 11

1. POLICY STATEMENT

KVA is committed to protecting the privacy, dignity and personal data of its members, employees, programme beneficiaries, research participants, partners and all other persons whose personal data it processes. Personal data collected by KVA shall be used lawfully, fairly, and transparently; for explicit and legitimate purposes; limited to what is necessary; kept accurate and secure; retained only as long as necessary; and transferred only with appropriate safeguards.

KVA shall embed data protection into programme design, membership administration, human-resource management, research, monitoring and evaluation, communications, events, digital systems and partner arrangements. Personal data shall not be collected merely because it may be useful in future.

2. SCOPE AND OBJECTIVES

Scope

This Policy applies to the collection, use, storage, sharing, retention and disposal of personal data by or on behalf of KVA.

It applies to personal data processed in paper or electronic form by NEC members acting for KVA, BEC Members acting for KVA, KVA Taskforces and Working Groups, KVA staff, consultants, interns, volunteers, attaches, contractors and partners. It covers, among other things, membership records; employee and recruitment records; programme and beneficiary data; research and survey data; photographs, video and audio; event registrations; stakeholder contacts; supplier and consultant information; payment records; website and digital-platform data; and complaints, safeguarding or incident records.

Objectives

The objectives of this policy include:

- Ensure personal data is collected and processed lawfully, fairly, transparently and only for defined purposes;
- Protect personal data through appropriate organisational, physical and technical safeguards;
- Provide practical procedures for consent, data-subject rights, sharing, retention, breach management and high-risk processing; and
- Promote accountability and compliance with applicable Kenyan data-protection requirements across KVA activities.

3. LEGAL AND REGULATORY FRAMEWORK

This Policy shall be implemented in accordance with the Constitution of Kenya, 2010, particularly the right to privacy; the Data Protection Act, 2019; the Data Protection (General) Regulations, 2021; the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021; the Data Protection (Complaints Handling and Enforcement Procedures) Regulations, 2021; and other applicable Kenyan laws, regulatory guidance and contractual requirements.

Where donor or partner requirements provide a higher level of protection, KVA may apply those requirements provided they do not reduce protections required by Kenyan law.

4. KEY DEFINITIONS

Term	Meaning
Personal data	Information relating to an identified or identifiable natural person.
Sensitive personal data	Personal data requiring enhanced protection, including data relating to health, race or ethnic origin, beliefs, genetic or biometric data, property or family details, sex or sexual orientation, and other categories recognized by law.
Data subject	The individual to whom personal data relates.
Processing	Any operation performed on personal data, including collection, recording, storage, use, analysis, sharing, transfer, alteration, retrieval, publication, archiving or deletion.
Data controller	An entity that determines the purpose and means of processing personal data.
Data processor	An entity that processes personal data on behalf of a controller.
Personal data breach	A security incident leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data.

5. DATA PROTECTION PRINCIPLES

KVA shall ensure that personal data is:

- Processed lawfully, fairly and transparently;
- Collected for explicit, specified and legitimate purposes and not used incompatibly with those purposes;
- Adequate, relevant and limited to what is necessary;
- Accurate and, where necessary, kept up to date;
- Retained in identifiable form only for as long as necessary;
- Protected through appropriate technical, organizational and physical safeguards; and
- Transferred outside Kenya only where lawful safeguards or other permitted conditions are in place.

6. GOVERNANCE AND RESPONSIBILITIES

6.1 National Executive Council (NEC)

The NEC approves this Policy and provides governance oversight over significant privacy risks, material breaches and organizational compliance.

6.2 Chief Executive Officer (CEO)

The Chief Executive Officer (CEO), or a designated person appointed in the absence of the CEO, is responsible for implementation, adequate resources, assignment of data-protection responsibilities, regulatory compliance and escalation of significant incidents.

6.3 Data Protection Officer / Designated Data Protection Focal Person

KVA CEO shall designate an appropriately competent person to coordinate data-protection compliance. Where appointment of a Data Protection Officer is required by law or determined appropriate by KVA, the appointment and functions shall comply with applicable requirements. The role includes advising staff, maintaining key compliance records, coordinating data-subject requests, supporting DPIAs, monitoring breaches and serving as a point of contact on data-protection matters.

6.4 Administrative officers

Admins shall integrate privacy into programme design and data-collection tools, minimize data collection, ensure appropriate notices and lawful bases, restrict access, manage processors and partners, and report incidents promptly.

6.5 All Personnel

All persons handling KVA personal data shall comply with this Policy, maintain confidentiality, use approved systems and devices, protect passwords and records, and immediately report suspected loss, misuse, unauthorized access or disclosure.

7. DATA INVENTORY, PURPOSE AND LAWFUL PROCESSING

KVA shall maintain an appropriate record or inventory of significant personal-data processing activities, identifying the data collected, categories of data subjects, purpose, lawful basis, recipients, storage location, retention period and any international transfer.

Before collecting personal data, the responsible team shall establish a lawful and documented reason for processing. Consent shall be used where appropriate, but KVA shall not rely on consent where another lawful basis is more suitable or where consent cannot be freely given. Where consent is relied upon, it shall be informed, specific, demonstrable and capable of being withdrawn.

8. COLLECTION, PRIVACY NOTICES AND DATA MINIMISATION

At or before collection, KVA shall provide an appropriate privacy notice or explanation describing, in clear language, who is collecting the data, the purpose of collection, relevant uses and recipients, whether provision is mandatory or voluntary, applicable rights, relevant retention or transfer information, and how the data subject can raise a concern. Where consent is the identified lawful basis, KVA shall request and document consent after providing this information.

Forms, surveys, membership systems and programme tools shall collect only information reasonably necessary for the stated purpose. Optional fields should be clearly identified where relevant. Collection of personal information requires particular justification and safeguards.

9. SENSITIVE DATA, CHILDREN AND VULNERABLE DATA SUBJECTS

Sensitive personal data shall be processed only where necessary, lawful and subject to enhanced safeguards. Access shall be limited to personnel who require it for authorised duties.

Where KVA processes personal data relating to children or persons who may require additional support to understand the processing, the responsible team shall apply applicable consent or

authorisation requirements, age-appropriate and accessible explanations, data minimisation and enhanced confidentiality. For children aged 12–17 years, KVA shall seek the child's assent in addition to parent/guardian consent where consent is the applicable basis and the child is capable of understanding the proposed processing, subject to applicable law, ethics approval and safeguarding requirements. Safeguarding and GEDI policy shall apply alongside this Policy where relevant.

10. RESEARCH, SURVEYS, PROGRAMME MONITORING AND BENEFICIARY DATA

Data collection shall be designed to minimize identifiable information and separate identifiers from analytical datasets where practicable.

- Survey and monitoring tools shall have a defined purpose and approved data fields.

Safeguarding and GEDI case information shall be managed under the Safeguarding and GEDI Policy for case response, while this Policy governs privacy, access and security. Whistleblowing reports and reporter identities shall be handled under KVA's Whistleblowing and Non-Retaliation arrangements, with this Policy applying to the personal data contained in those records. Financial-crime investigations remain governed by the Financial Crime Prevention Policy 2026.
This Policy is the primary KVA policy for privacy and personal-data processing. The Records Management and Retention Policy governs how long official records are kept and how they are archived or destroyed; where a record contains personal data, both policies apply and the more protective lawful requirement shall be followed.

POLICY INTERACTION AND REFERRAL

- Research data shall comply with applicable ethical approvals, participant information and consent requirements.
- Unique identifiers, coding, aggregation or anonymization should be used where direct identification is unnecessary.
- Field teams shall not leave completed forms, participant lists or devices containing personal data unattended.
- Personal contact details collected for programme implementation shall not automatically be used for unrelated communications, publicity or fundraising.
- Donor reporting should use aggregated or anonymized information unless identifiable information is necessary and lawfully permitted.

11. PHOTOGRAPHS, VIDEO, AUDIO, STORIES AND COMMUNICATIONS

KVA shall consider privacy and safeguarding before capturing or publishing identifiable photographs, video, audio, testimonials or beneficiary stories. Individuals shall receive sufficient information about the intended use and distribution, and consent/Assent or another appropriate lawful basis shall be documented where required.
Special care shall be taken with children, vulnerable persons, health information, precise locations and stories that could expose an individual to stigma, discrimination, retaliation or other harm. Consent to receive a programme service shall not be treated automatically as consent for publicity.

12. DATA QUALITY, ACCESS AND SECURITY

KVA shall take reasonable steps to keep personal data accurate and protect it against loss, theft, unauthorized access, alteration, disclosure or destruction. Safeguards shall be proportionate to the sensitivity, volume and risks of the data.

- Role-based or need-to-know access;
- Strong passwords and, where available, multi-factor authentication;
- Screen locking and secure device configuration;
- Approved storage and file-sharing locations;
- Secure backups for critical records;
- Encryption or equivalent safeguards where warranted by risk;
- Locked storage for paper records and controlled access to offices or archives;
- Secure disposal of paper (through burning or shredding) and electronic records (through permanent deletion);
- Confidentiality obligations for personnel and relevant service providers; and
- Timely removal or modification of access when roles change or personnel leave KVA.

13. SHARING, PROCESSORS, PARTNERS AND INTERNATIONAL TRANSFERS

Personal data shall be shared only where necessary, lawful and proportionate. Before sharing identifiable data with a consultant, service provider, implementing partner, donor or other third party, KVA shall confirm the purpose, minimum data required, security arrangements, permitted uses, retention and deletion requirements, and responsibility for responding to incidents or data-subject requests.

Where a third-party processes personal data on KVA's behalf, appropriate contractual data-protection provisions shall be used. International transfers shall occur only where the requirements of Kenyan law are satisfied, including appropriate safeguards or other legally permitted grounds. Sensitive personal data shall receive the additional protection required by law.

14. DATA RETENTION AND SECURE DISPOSAL

KVA shall not retain identifiable personal data indefinitely. Retention periods shall reflect legal, contractual, operational, research, financial and accountability requirements. Where there is no continuing lawful need, records shall be securely deleted, destroyed or irreversibly anonymized.

A retention schedule shall be maintained for major record categories. A legal hold, audit, investigation or active dispute may justify temporary suspension of routine disposal. All data in electronic devices shall be permanently destroyed before such devices are disposed of

15. DATA SUBJECT RIGHTS AND REQUESTS

KVA shall respect rights available to data subjects under applicable law, including rights relating to information, access, objection to processing, correction of inaccurate or misleading data, and deletion of false or misleading data, together with any other rights applicable to the particular processing.

Requests shall be forwarded promptly to the designated data-protection contact, verified appropriately, recorded and handled within applicable legal timelines. KVA shall not require excessive information to verify identity and shall document any lawful reason for refusing or restricting a request.

16. DATA PROTECTION IMPACT ASSESSMENTS AND PRIVACY BY DESIGN

Privacy shall be considered before introducing new systems, technologies, datasets or programme activities. A Data Protection Impact Assessment (DPIA) shall be undertaken where proposed processing is likely to present high risk to the rights and freedoms of individuals, including relevant large-scale, sensitive, biometric, genetic, profiling or other high-risk processing.

The DPIA shall describe the proposed processing, assess necessity and proportionality, identify privacy risks, document safeguards and determine whether residual risk is acceptable before processing begins.

17. PERSONAL DATA BREACH MANAGEMENT

Any person who becomes aware of an actual or suspected personal data breach shall immediately report it to the designated KVA data-protection contact and responsible manager. Personnel shall not conceal, independently investigate, delete evidence or communicate externally about a breach unless authorized.

KVA shall promptly contain the incident, preserve relevant information, assess the data and persons affected, evaluate likely harm, document decisions, implement corrective action and make required notifications. Where KVA acts as a data controller and a breach presents a real risk of harm to a data subject, notification to the Office of the Data Protection Commissioner shall be made within the legally applicable period. Where KVA acts as a processor, it shall notify the relevant controller without undue delay and within applicable legal requirements.

Where required, affected data subjects shall be informed in clear language about the nature of the breach, likely consequences, measures taken and practical steps they can take to protect themselves.

18. REGISTRATION, TRAINING, MONITORING AND COMPLIANCE

KVA shall determine and maintain any registration required with the Office of the Data Protection Commissioner as a data controller and/or data processor, taking account of its processing activities and applicable registration requirements.

Personnel with access to personal data shall receive appropriate induction and periodic awareness on confidentiality, secure handling, phishing and password risks, beneficiary privacy, breach reporting and data-subject rights. Compliance shall be monitored through periodic review of data inventories, access rights, retention, processor arrangements, incidents, DPIAs and programme practices.

Deliberate or negligent misuse of personal data may result in corrective or disciplinary action in accordance with KVA procedures and applicable law.

19. COMPLAINTS AND ESCALATION

Individuals may raise a privacy or data-protection concern through the KVA Secretariat or designated contact focal point. Matters that are primarily safeguarding, GEDI, whistleblowing or financial-crime concerns shall be referred to the responsible policy pathway while any personal data continues to be protected under this Policy. Privacy complaints shall be acknowledged, assessed fairly, handled confidentially and documented. Nothing in this Policy prevents a data subject from exercising the right to lodge a complaint with the Office of the Data Protection Commissioner or pursue another remedy available by law.

20. RECORD KEEPING AND POLICY REVIEW

KVA shall maintain proportionate records demonstrating compliance, including relevant processing inventories, privacy notices and consent records, data-sharing or processing agreements, data-subject requests, DPIAs, breach records, training records, retention schedules and corrective actions.

This Policy shall normally be reviewed every three years or earlier following significant legal or regulatory change, significant changes to KVA processing activities or technology, a serious data breach, audit findings or NEC direction.

21. APPROVAL AND AUTHORISATION

This Policy becomes effective upon approval by the National Executive Council of the Kenya Veterinary Association.

Approval item	**Details**
Approval date	Wednesday, 16th September 2026
Effective date	Thursday, 17th September 2026
Next scheduled review	Monday, 17th September 2029
Policy version	1.0

President

Name: _**DR. KELVIN OSORE**_____

Signature: __  _____

Date: __**THURSDAY, 17TH SEPTEMBER 2026.** _____

— END —

ANNEX

ANNEX 1: PERSONAL DATA PROCESSING REGISTER

Use this register to document significant categories of personal data processed by KVA.

Processing activity	Data subjects / data	Purpose & lawful basis	Recipients / processor	Storage & security	Retention / transfer

ANNEX 2: PRIVACY AND DATA COLLECTION CHECKLIST

Check	Yes	No/N/A	Comments / action
Purpose for collecting the data is clear and documented.	☐	☐	
Only necessary data fields are included.	☐	☐	
Lawful basis for processing has been identified.	☐	☐	
Privacy notice / participant information is ready.	☐	☐	
Consent mechanism is appropriate where consent is relied upon.	☐	☐	
Sensitive data is justified and enhanced safeguards are defined.	☐	☐	
Children or vulnerable participants have been considered.	☐	☐	
Access is limited to authorized personnel.	☐	☐	
Storage and transfer arrangements are secure.	☐	☐	
Retention period and disposal method are defined.	☐	☐	
Third-party processors or partners have appropriate safeguards.	☐	☐	
International transfer requirements have been considered.	☐	☐	
DPIA screening has been completed where the activity may present high privacy risk.	☐	☐	

ANNEX 3: DATA SUBJECT REQUEST FORM AND REGISTER

Request details	***Information***
Request reference	_____
Date received	_____
Name / contact of requester	_____
Request type	☐ Information ☐ Access ☐ Correction ☐ Objection ☐ Deletion ☐ Other
Identity / authority verified	☐ Yes ☐ No ☐ Not yet
Description of request	
Responsible officer	_____
Due / response date	_____
Decision / action taken	
Date closed	_____

ANNEX 4: PERSONAL DATA BREACH REPORT FORM

Incident information	Details
Breach reference	_____
Date/time discovered	_____
Reported by	_____
System / programme / location	_____
What happened	
Categories of personal data affected	
Approximate number / categories of data subjects	
Sensitive personal data involved?	☐ Yes ☐ No ☐ Unknown
Immediate containment action	
Likely consequences / risk of harm	
Controller / processor role	☐ KVA controller ☐ KVA processor ☐ To be confirmed
External notification required?	☐ ODPC ☐ Data subject(s) ☐ Partner/controller ☐ Other ☐ Not required
Notification date / reference	
Corrective actions and owner	
Closure / lessons learned	

ANNEX 5: DATA PROTECTION IMPACT ASSESSMENT (DPIA) SCREENING

If one or more high-risk indicators apply, seek advice from the designated data-protection contact on whether a full DPIA is required before processing begins.

High-risk indicator	Yes	No	Comments
Large-scale processing of personal or sensitive personal data.	☐	☐	
Biometric or genetic data.	☐	☐	
Automated decision-making, profiling or scoring with significant effects.	☐	☐	
New technology or a new use of existing technology involving personal data.	☐	☐	
Systematic monitoring, tracking or precise location data.	☐	☐	
Combining datasets from different sources in a way that increases privacy risk.	☐	☐	
Processing involving children or other vulnerable persons.	☐	☐	
Use of data for a materially different purpose from the original collection.	☐	☐	
International transfer involving significant volumes or sensitive data.	☐	☐	
Processing where a breach could cause serious physical, financial, reputational or social harm.	☐	☐	

Screening outcome: ☐ Full DPIA required ☐ Full DPIA not required ☐ Further advice required

Reviewed by: _____ Date: _____

ANNEX 6: DATA RETENTION SCHEDULE TEMPLATE

Record category	Owner	Retention period / trigger	Reason / authority	Final action
Membership records				
HR / recruitment records				
Programme beneficiary records				
Research / survey data				
Financial / supplier records				
Event / training records				
Communications / media consent records				
Complaints / safeguarding / incident records				
Other: _____				

ANNEX 7: THIRD-PARTY DATA SHARING / PROCESSOR DUE-DILIGENCE CHECKLIST

Due-diligence item	Yes	No/N/A	Comments / action
Purpose and necessity of sharing are documented.	☐	☐	
Only the minimum necessary data will be shared.	☐	☐	
Controller / processor roles are clear.	☐	☐	
Recipient has appropriate technical and organisational safeguards.	☐	☐	
Confidentiality obligations are in place.	☐	☐	
Processing instructions and permitted uses are documented.	☐	☐	
Sub-processors require appropriate authorisation and safeguards.	☐	☐	
Incident / breach notification responsibilities are defined.	☐	☐	
Data-subject request cooperation is defined.	☐	☐	
Retention, return and secure deletion requirements are defined.	☐	☐	
International transfer requirements have been assessed.	☐	☐	
Contract / data-processing agreement has been approved where required.	☐	☐	

Reviewed / approved by: _____ Date: _____

ANNEX 8: PERSONAL DATA CONSENT AND MEDIA PERMISSION FORM

Use this form only where consent is the identified lawful basis for the relevant processing. Consent for one purpose does not automatically constitute consent for another purpose.

A. Participant / Data Subject Details

Name: _____ Role/Organisation (if applicable): _____
Programme/Event/Activity: _____ Date: _____

B. Information KVA May Collect

Tick the categories that apply:
☐ Name and identification/contact details
☐ Membership, professional, employment or organisational details
☐ Programme, training, event, survey or research responses
☐ Payment or reimbursement details, where required
☐ Health or other sensitive personal data, only where specifically necessary and explained
☐ Photograph/image
☐ Video recording
☐ Audio/voice recording
☐ Testimonial, quotation, caption or personal story
☐ Other: _____

C. Purpose and Intended Use

Purpose(s) explained to the participant: _____
Intended recipients/platforms, where applicable:
_____
Retention period or review point, where known:
_____

D. Consent Choices

Please tick the choices that apply:
☐ I CONSENT to KVA collecting and using the non-media personal data identified above for the stated purpose(s).
☐ I DO NOT CONSENT to optional non-media processing based on consent.
☐ I CONSENT to KVA capturing and using my photograph, video, audio, testimonial/story or related media for the stated KVA reporting, education, communication, advocacy or approved promotional purpose(s).
☐ I DO NOT CONSENT to photography, video, audio or media use based on consent.
I understand that I may withdraw consent for future processing where consent is the lawful basis, without affecting processing already lawfully undertaken before withdrawal.

E. Children Aged 12–17 Years, Where Applicable

Parent/Guardian consent: ☐ Yes ☐ No Name: _____ Signature: _____ Date: _____
Child assent: ☐ Yes ☐ No Child name: _____ Signature/mark: _____ Date: _____
The information shall be explained in age-appropriate language. Refusal by the child shall be respected unless another lawful basis or safeguarding/legal requirement applies.

F. Confirmation and Contact

Data subject/participant name: _____ Signature/mark: _____ Date: _____
KVA representative obtaining consent: _____ Signature: _____ Date: _____

Questions, withdrawal requests or privacy concerns should be directed to the KVA Data Protection Officer / designated Data Protection Focal Person through the approved KVA contact channels.