KENYA VETERINARY ASSOCIATION (KVA)

RECORDS MANAGEMENT AND RETENTION POLICY

DOCUMENT CONTROL

Field	Details
Document title	KVA Records Management and Retention Policy
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	All KVA staff, NEC members, BEC Members, KVA Members, consultants, interns, volunteers, contractors and partners who create, receive, use, store or dispose of KVA records.
Review cycle	Every three years from latest effective date, or earlier following legal, operational or technological change, audit findings, a significant records incident or NEC direction.

VERSION CONTROL

Version	Date	Summary of changes	Approved by
1.0	17/9/26	Initial policy for approval	NEC

RELATED KVA POLICIES AND PROCEDURES

- Data Protection Policy and Procedures
- Health, Safety and Wellbeing Policy and Procedures
- Safeguarding Policy and Procedures
- Human resource and staff conduct procedures
- Finance and procurement procedures
- ICT / information-security procedures, where applicable
- Research, monitoring, evaluation and learning procedures

TABLE OF CONTENTS

1. POLICY STATEMENT

KVA shall create, maintain, protect and dispose of records in a systematic manner so that reliable evidence of its governance, membership, programmes, finances, employment, partnerships and decisions is available when required. Records shall be authentic, accurate, complete, accessible to authorised users and protected against unauthorised alteration, loss, disclosure or destruction.

Records shall be retained only for as long as required by law, contract, donor conditions, operational need, accountability or legitimate institutional value. Personal data shall not be retained indefinitely merely because storage is available.

2. PURPOSE AND SCOPE

This Policy establishes KVA's framework for records creation, classification, filing, access, storage, retention, archiving and secure disposal. It applies to records in all formats and locations, including paper files, email, shared drives, cloud platforms, databases, messaging platforms used for official business, photographs, audio/video, survey systems and records held by third parties on KVA's behalf.

It covers governance and NEC records; membership records; finance and procurement; human resources; programmes and grants; research and MEL; contracts and partnerships; communications and publications; safeguarding, complaints and incidents; legal and regulatory records; ICT records; and other evidence of KVA business.

3. LEGAL AND POLICY FRAMEWORK

This Policy shall be implemented in accordance with applicable Kenyan law and KVA obligations, including the Data Protection Act, 2019 and the Data Protection (General) Regulations, 2021; the Societies Act (where applicable to KVA's registration and statutory records); the Tax Procedures Act, 2015; the Employment Act, 2007; applicable public-health, research, contractual and donor requirements; and any lawful preservation, audit or regulatory directions.

Where different requirements apply to the same record, KVA shall normally follow the longest applicable lawful retention period unless legal advice or a competent authority directs otherwise.

4. DEFINITIONS

Term	Meaning
Record	Recorded information created, received or maintained as evidence of KVA activities, decisions, obligations or transactions, regardless of format.
Official record	The authoritative version that KVA relies on as evidence of a transaction, decision or activity.
Working document	A temporary draft, duplicate or convenience copy that is not the official record and has no continuing business or evidential value.
Retention period	The period for which a record must be kept before authorised disposal, review or permanent preservation.

Archive	Records preserved for long-term or permanent institutional, governance, historical or evidential value.
Legal hold	A temporary suspension of normal disposal because records may be relevant to litigation, investigation, audit, complaint or regulatory action.
Disposal	Authorised destruction, deletion, anonymisation or transfer to permanent archives at the end of the retention period.

5. RECORDS MANAGEMENT PRINCIPLES

- Accountability: KVA shall be able to demonstrate significant decisions, transactions and programme actions.
- Authenticity and integrity: official records shall be protected from unauthorised alteration and their origin and context should be clear.
- Accessibility: authorised users shall be able to locate and retrieve records when needed.
- Confidentiality and security: access shall be proportionate to sensitivity and business need.
- Data minimisation: unnecessary personal data and duplicate records shall not be retained.
- Lifecycle management: retention and disposal requirements shall be considered from creation, not only when storage becomes full.
- Consistency: official records shall be stored in approved locations using agreed naming and filing practices.

6. ROLES AND RESPONSIBILITIES

6.1 National Executive Council (NEC)

The NEC approves this Policy and oversees significant records-management risks, including preservation of core governance and institutional records.

6.2 Honorary Secretary/Chief Executive Officer (CEO)

The Honorary Secretary/Chief Executive Officer (CEO) is accountable for implementation, assignment of responsibilities, adequate systems and resources, and compliance with legal, contractual and donor requirements.

6.3 Records Management Focal Person / Secretariat

The designated focal person shall maintain the records classification and retention schedule, coordinate periodic disposal and archiving, support retrieval, maintain disposal records and advise teams on filing and retention.

6.4 Department, Programme and Project Leads

Managers are responsible for ensuring that official records from their functions and projects are captured in approved locations, appropriately classified, protected and handed over at project or staff transition.

6.5 All Personnel

Personnel shall create adequate records of official business, use approved storage locations, follow naming and access rules, protect confidential records and not destroy, remove or privately retain official KVA records without authority.

7. RECORD CREATION, CAPTURE AND FILING

Safeguarding, GEDI, whistleblowing, non-retaliation and financial-crime case files are restricted records. Their case-management rules are governed by the relevant substantive policy, while this Policy governs secure custody, retention, legal holds and authorised disposal. Legal holds, active investigations, audits, donor requirements and statutory obligations override routine disposal.

This Policy governs the lifecycle of KVA official records. The Data Protection Policy governs the lawful processing and protection of personal data within those records. A retention period in this Policy does not authorise KVA to retain unnecessary personal data where law requires earlier deletion or anonymisation, and a data-protection deletion request does not require destruction of a record that KVA must lawfully preserve.

POLICY INTERACTION AND REFERRAL

KVA shall maintain sufficient records to document significant decisions, approvals, transactions, commitments, programme delivery and statutory obligations. An official record should be captured promptly in the appropriate KVA repository rather than remaining only in an individual's inbox, personal device or messaging account.

- Final signed or approved versions shall be distinguishable from drafts.
- Meeting minutes shall identify the meeting, date, participants where appropriate, decisions and actions.
- Contracts, grant agreements, approvals and significant correspondence shall be filed with the related project or functional record.
- Records received through WhatsApp or similar channels that constitute material approvals, decisions or evidence shall be transferred to the relevant official file or repository.
- File names should be meaningful and, where useful, include the subject, date and version.
- Unnecessary duplicates and transitory drafts should be removed when no longer needed.

8. RECORDS CLASSIFICATION AND FILE STRUCTURE

The Secretariat shall maintain a practical classification structure so that records are organised by business function rather than by individual staff member. At minimum, KVA repositories should distinguish governance; membership; finance; HR; programmes/projects; research and MEL; procurement and contracts; partnerships; communications; safeguarding/complaints; legal/regulatory; and ICT/administrative records.

Sensitive and restricted records shall be stored separately or protected through access controls where necessary.

9. STORAGE, ACCESS AND SECURITY

Official electronic records shall be stored in KVA-approved systems or repositories with appropriate access controls and backup arrangements. Paper records shall be stored in suitable cabinets or secure areas, with restricted access for confidential files.

- Access shall be based on role and legitimate business need.
- Shared passwords and uncontrolled public links should be avoided.
- Sensitive records shall not be routinely stored on personal email accounts or unmanaged personal devices.
- Where removable media is necessary, it shall be protected and controlled according to risk.
- Records taken to field activities shall be limited to what is necessary and returned or securely transferred after use.
- Access shall be reviewed when staff, consultants or office bearers change roles or leave KVA.

10. EMAIL, MESSAGING AND DIGITAL COLLABORATION

Email and messaging platforms are communication tools, not permanent filing systems. Messages that document significant decisions, approvals, contractual commitments, programme evidence or other official business shall be saved or transferred to the appropriate KVA record location.

Staff shall avoid conducting substantive KVA business exclusively through personal accounts. Where circumstances require use of a personal device or account, the official record shall be transferred to KVA custody as soon as practicable.

11. PROJECT, RESEARCH AND PROGRAMME RECORDS

Each programme or project shall maintain an orderly record from inception to close-out. The project file should, as applicable, contain the proposal and agreement, approved budget and amendments, workplans, approvals, procurement and contracts, participant or beneficiary records, field tools, datasets, ethics or regulatory approvals, monitoring evidence, deliverables, reports, financial records, correspondence, donor feedback and close-out documentation.

Research datasets shall be managed in accordance with ethical approvals, consent commitments and the KVA Data Protection Policy. Identifiers should be separated or removed where continued identification is unnecessary.

12. RECORD RETENTION

The retention schedule in Annex 1 establishes KVA's default minimum periods. A record shall be retained longer where required by law, an active donor or contract, an audit, insurance requirement, research protocol, investigation, complaint, dispute or legal hold.

For personal data, retention shall remain tied to a lawful purpose. The Data Protection (General) Regulations require organisations to establish retention schedules, periodically review whether continued storage is necessary, and delete, erase, anonymise or pseudonymise personal data when its purpose has lapsed, subject to lawful reasons for continued retention.

13. ARCHIVES AND PERMANENT RECORDS

Records with enduring governance, legal, historical or institutional value shall be preserved as KVA archives rather than destroyed. These normally include the constitution and major amendments; registration and foundational records; approved policies; AGM and NEC approved minutes; audited annual financial statements; annual reports; major strategic plans; records of office bearers; significant institutional agreements; major publications; and selected records documenting KVA's history and professional contribution.

Permanent archives containing personal data shall remain subject to appropriate access restrictions and data-protection safeguards.

14. DISPOSAL AND DESTRUCTION

Records shall be disposed of only after the applicable retention period has expired, no legal hold or other preservation requirement applies, and disposal has been authorised. Disposal shall be appropriate to the sensitivity of the information.

- Confidential paper shall be shredded or otherwise destroyed so it cannot reasonably be reconstructed.
- Electronic records shall be securely deleted from active systems and, where practicable, from routine storage in accordance with system capabilities and backup cycles.
- Storage devices containing confidential information shall be securely wiped or physically destroyed before disposal or reuse where appropriate.
- Routine duplicates, convenience copies and transitory records may be deleted without a formal disposal process once they no longer have business value, provided the official record is preserved.

Formal disposal of scheduled official records shall be documented in a Records Disposal Register.

15. LEGAL HOLDS, AUDITS AND INVESTIGATIONS

Normal destruction shall stop immediately for records reasonably relevant to anticipated or ongoing litigation, regulatory inquiry, audit, investigation, safeguarding matter, complaint, insurance claim or other formal dispute. The Chief Executive Officer (CEO) / Head of Secretariat or authorised officer shall communicate the hold, its scope and its release. Records under hold shall not be altered or destroyed even if their normal retention period expires.

16. STAFF, CONSULTANT AND OFFICE-BEARER TRANSITIONS

Before separation, change of role or completion of an assignment, personnel shall hand over official KVA records, files, credentials and relevant working materials to the responsible manager or Secretariat. KVA records shall not be deleted, removed or retained as personal copies merely because an individual created them.

Access rights shall be reviewed promptly and records held in individual accounts or devices shall be transferred where necessary for continuity.

17. THIRD PARTIES, CONTRACTORS AND CLOUD SERVICES

Contracts with service providers that create, host, digitise, store or destroy KVA records shall address confidentiality, security, ownership/custody, access, backup, return or transfer of records, retention and secure deletion as appropriate. KVA shall remain able to retrieve its official records during and at the end of the arrangement.

Where records contain personal data, the KVA Data Protection Policy and applicable processor or data-sharing requirements shall also apply.

18. MONITORING, REVIEW AND NON-COMPLIANCE

The Secretariat shall periodically review filing practices, access permissions, retention schedules, storage risks, project close-out files and disposal activity. Record owners may be required to correct incomplete filing, excessive duplication, unauthorised storage or overdue disposal.

Unauthorised destruction, concealment, alteration, removal or disclosure of KVA records may result in corrective or disciplinary action and, where applicable, referral under contractual or legal procedures.

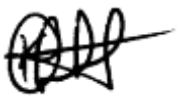
19. POLICY REVIEW

This Policy shall normally be reviewed every three years or earlier following material changes in law, KVA operations, information systems, donor requirements, audit findings, a significant records or data incident, or NEC direction.

20. APPROVAL AND AUTHORISATION

This Records Management and Retention 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: KVA RECORDS RETENTION SCHEDULE

The periods below are KVA default minimums. “Permanent” means preserve as an institutional archive. Where law, donor terms, contract, ethics approval, audit, investigation or legal hold requires longer retention, the longer requirement applies. Personal data should be minimised or anonymised where continued identification is unnecessary.

Record category	Examples	Default retention	Final action / notes
Governance and constitutional	Constitution; registration; AGM and NEC approved minutes; resolutions; election records; approved policies; strategic plans	Permanent	Archive authoritative version; restrict confidential supporting papers as appropriate.
Membership master register	Member name, contact, admission/cessation status and core membership history	Life of membership + 7 years; retain minimal historical membership register permanently where required for institutional/statutory record	Remove unnecessary personal details after active need ends; preserve statutory/core membership evidence.
Routine membership administration	Applications, subscription correspondence, routine member service records	7 years after closure/cessation	Destroy securely unless required for dispute, audit or historical record.
Audited financial statements and annual reports	Signed audited accounts; final annual reports	Permanent	Institutional archive.
Accounting, tax and transaction records	Ledgers, invoices, receipts, vouchers, bank records, payroll tax records, reconciliations	7 years after end of relevant financial year	KVA policy exceeds the general five-year tax-record minimum; retain longer if tax matter or proceeding remains open.

Procurement records	Quotations, bids, evaluations, purchase orders, tender records	7 years after completion/close-out	Longer where donor/contract requires.
Contracts and agreements	Donor agreements, MOUs, leases, consultant/vendor contracts	7 years after expiry/termination	Permanent for agreements of exceptional institutional significance; retain longer for unresolved claims.
HR personnel files	Contracts, leave, performance, disciplinary and separation records	7 years after separation	Retain only necessary employment record; health/sensitive information separately protected.
Recruitment - unsuccessful candidates	Applications, CVs, interview notes	2 years after recruitment closes	Delete securely unless consent/lawful purpose supports a talent pool or dispute requires retention.
Payroll and benefits supporting records	Payroll schedules, statutory deductions, benefit administration	7 years	Coordinate with financial/tax records.
Programme / project core file	Agreement, approved proposal/budget, workplans, key approvals, deliverables, reports, close-out	7 years after project close, or donor period if longer	Archive selected major programme records of enduring institutional value.
Programme financial/supporting records	Project vouchers, procurement, expense support, timesheets where applicable	7 years after project/financial year close, or donor period if longer	Subject to audit and donor requirements.

Beneficiary / participant identifiable records	Registration lists, contacts, attendance, service records	Purpose-specific; normally project duration + up to 5 years where needed for accountability	Delete/anonymise earlier when identification is no longer necessary; longer only with documented lawful basis.
Research source data and identifiable datasets	Consent forms, coded link files, identifiable research data	As specified by ethics approval/protocol/donor; otherwise 5 years after study close as a default review point	Anonymise where feasible; consent forms may need separate retention from datasets.
Anonymised research datasets	De-identified datasets with no reasonable means of re-identification	As required for scientific/institutional value	May be archived long-term where ethically and contractually permitted.
Training and event records	Agendas, participant lists, attendance, evaluations	5 years after event/project close	Keep final reports/materials longer where institutionally useful; minimise contact data.
Communications and publications	Final publications, press releases, approved campaigns, major media outputs	Permanent for final institutional publications; 3 years for routine working files	Archive final public outputs.
Photo/video/audio consent and media files	Consent forms, identifiable media, beneficiary stories	Duration of approved use + 3 years, then review	Withdraw/remove from active use where consent is withdrawn and no other lawful basis applies; archive only where justified.

Safeguarding, complaints and serious incident records	Case files, investigations, referrals, outcomes	Minimum 7 years after closure, with a case-specific review; retain longer where required for child safeguarding, serious misconduct, legal, donor or regulatory reasons	Highly restricted access; longer retention may be required for serious or continuing matters.
Legal claims and disputes	Legal correspondence, pleadings, evidence, settlement records	7 years after final closure, or as advised by counsel	Legal hold overrides routine disposal.
Insurance records and claims	Policies, claims, supporting evidence	7 years after expiry/claim closure	Longer for unresolved or long-tail claims where advised.
ICT access and security records	User access approvals, significant security logs/incidents	2 years after access ends / incident closes, unless risk or investigation requires longer	Security logs may have shorter system-specific periods documented by ICT.
Routine correspondence and administrative records	Routine scheduling, logistics, non-substantive email	2 years or until administrative purpose ends	Delete where no continuing business value.
Drafts, duplicates and transitory material	Superseded drafts, duplicate copies, convenience downloads	Until superseded or purpose ends	Delete routinely once official record is captured.

ANNEX 2: RECORDS DISPOSAL AUTHORISATION AND REGISTER

Field	Details
Disposal reference	_____
Department / project	_____
Record series / category	_____
Date range of records	_____
Retention requirement met	☐ Yes ☐ No
Legal hold / audit / investigation checked	☐ Clear ☐ Hold applies
Personal data involved	☐ Yes ☐ No
Proposed disposal method	☐ Shred ☐ Secure delete ☐ Anonymise ☐ Archive transfer ☐ Other
Quantity / location	_____
Authorised by	_____
Disposal date	_____
Disposed / witnessed by	_____
Comments / certificate reference	

ANNEX 3: PROJECT / PROGRAMME RECORDS CLOSE-OUT CHECKLIST

Close-out check	Yes	No/N/A	Comments / action
Signed grant/contract and amendments filed.	☐	☐	
Final approved proposal, budget and workplan filed.	☐	☐	
Key approvals and decision records captured.	☐	☐	
Procurement and consultant/vendor records complete.	☐	☐	
Financial supporting records complete and reconciled.	☐	☐	
Final technical and financial reports filed.	☐	☐	
Participant/beneficiary records reviewed for retention and data minimisation.	☐	☐	
Research/MEL datasets and tools transferred to approved repository.	☐	☐	
Ethics, regulatory and consent records filed where applicable.	☐	☐	
Photographs/media and consent records reviewed.	☐	☐	
Donor retention period and audit requirements recorded.	☐	☐	
Outstanding complaints, incidents, claims or legal holds identified.	☐	☐	
Duplicate/transitory working files removed.	☐	☐	
Access permissions reviewed and former project-team access removed.	☐	☐	
Records owner and final storage location documented.	☐	☐	

Project/Programme: _____ Reviewed by: _____

Date: _____

ANNEX 4: RECORDS HANDOVER CHECKLIST

Use when a staff member, consultant, project lead or office bearer leaves or changes role.

Handover item	Completed / details
Official paper files returned / transferred	☐ Yes ☐ N/A Location: _____
Electronic project/department files transferred to approved repository	☐ Yes ☐ N/A
Material approvals/records from email or messaging captured	☐ Yes ☐ N/A
Passwords/credentials handled through approved IT process (not shared informally)	☐ Yes ☐ N/A
KVA devices, storage media and keys returned	☐ Yes ☐ N/A
Outstanding records, actions, audits, complaints or legal holds disclosed	☐ Yes ☐ N/A
Access rights identified for closure/change	☐ Yes ☐ N/A
Personal copies of confidential KVA records deleted/returned as required	☐ Yes ☐ N/A
Receiving officer	_____
Outgoing person	_____
Date	_____

ANNEX 5: RECORDS INVENTORY TEMPLATE

Business function	Record series	Format / system	Record owner	Access level	Retention	Disposition

ANNEX 6: LEGAL HOLD NOTICE TEMPLATE

A legal hold suspends normal deletion or destruction for records potentially relevant to a dispute, audit, investigation, complaint or regulatory matter.

Field	Details
Hold reference	_____
Matter / reason	_____
Date issued	_____
Records / date range covered	
Persons / teams affected	
Required action	Preserve all covered records. Do not delete, alter, overwrite or dispose of them until the hold is formally released.
Issued by	_____
Review date	_____
Release date / authority	_____