DATA PROTECTION POLICY

1. **Purpose**
   The purpose of this policy is to provide guidelines relating to the processing of personal data by the Kenya Red Cross Society (hereinafter referred to as "the Society").
2. **Scope**
   This policy covers data collected, received and stored on the Society owned physical and electronic databases and resource centre. It shall apply to all staff, volunteers and members of the Society, its Regions and County Branches. It shall also apply to all users of the Society's applications, software, databases, websites, social media platforms and all other suchlike resources.
   This policy shall cover all data/ information collection tools of the Society including but not being limited to assessment tools, membership databases, beneficiary databases, volunteer databases, EOC databases, mobile applications, research publications and communication tools such as photos, videos, social and main stream media.
3. **Definitions**
   - 3.1. **Consent** means any freely given, unambiguous and informed indication by a statement or by a clear positive action, signifies an agreement by the user to the processing of his/her personal data
   - 3.2. **Data controller** means a natural or legal person, public authority, agency or other body which has authority to oversee the management of, and to determine the purposes for the processing of personal data.
   - 3.3. **Data processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller
   - 3.4. **Data processing** means converting of data into information. This includes collecting, recording, rationalizing, storage, alteration, retrieval, use, transmission, dissemination, erasure or destruction of data.
   - 3.5. **Data subject** means an individual whose personal data is subject to processing
   - 3.6. **Data transfer** means all acts that make personal data accessible to third parties outside of the Society on paper, via electronic means, on internet or through other means.
   - 3.7. **Data Transfer Agreement** means an agreement between the Society and a third party that states the terms and conditions of use of personal data, including which data components are to be shared, the mode of transfer, how the data may be used, data security measures and other related issues.
   - 3.8. **Personal data** means any data related to a user who can be identified from that data; from that data and other information; or by means reasonably likely to be used related to that data. Personal data includes biographical data (bio data) such as name, sex, date of birth, country of origin, Identification Number as well as blood type.
   - 3.9. **Personal data breach** means a breach of data security leading to the accidental or unlawful/illegitimate destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transferred, stored or otherwise processed.
   - 3.10. **Person of concern** means a person whose protection and assistance needs are of interest to the Society.
   - 3.11. **Processing of personal data** means any operation, or set of operations, automated or not, which is performed on personal data, including but not limited to the collection, recording, organization, structuring, storage, adaption or alteration, retrieval, consultation, use, transfer, dissemination or otherwise making available, correction, or destruction.
   - 3.12. **Third party** means any natural or legal person other than the user. Examples of third parties are national governments, international governmental or non-governmental organizations, private sector entities or individuals.
4. **Policy guidelines**

4.1. The Society shall in dealing with personal information and data ensure that the information/ data is processed
   a) without infringing the privacy rights of the data subject;
   b) in a lawful manner; and
   c) in a reasonable manner

4.2. The collection, use, storage and transfer of personal data will only be done in a manner guided by the fundamental principles of the Red Cross Red Crescent Movement.

4.3. This policy will guide the KRCS ICT Acceptable Use Policy, the Record Retention and Destruction Policy and the Accountability Framework.

5. Accuracy

5.1. The Society shall store personal data/information as accurately as possible and update and systematically review it to ensure it fulfills the purpose(s) for which it is processed.

5.2. The data subject may request the correction of personal data that is inaccurate, incomplete, unnecessary or excessive.

5.3. When personal data is corrected, the Society will notify, as soon as is reasonably practicable, all third parties to whom the relevant personal data was transferred and to the data subject.

6. Lawful and fair processing

6.1. Data processing shall be carried out in a lawful and fair manner for specified and legitimate purposes without prejudicing the fundamental rights and freedoms of data subjects.

6.2. The processing shall only be justified based on one (or more) of the legal basis including:
   a) data subject giving his or her consent
   b) the processing is necessary for the performance of a contract with the data subject
   c) to meet legal compliance obligations
   d) to protect the data subject's vital interests or any other person who may be indirectly affected
   e) public interest
   f) to pursue the Society's legitimate interests which are not overridden because the processing prejudices the interests or fundamental rights and freedoms of data subjects

7. Further processing

7.1. Further processing for research purposes shall be compliant with the conditions outlined in order to be compatible with the purposes for which the data is obtained.

7.2. Personal data which is processed for research purposes may be exempt from provisions of this policy if the results of the research and statistical data is not made available in a form which identifies the data subject.

7.3. Further processing of data shall comply with the data protection principles set out in this policy, in particular in ensuring the security and confidentiality of sensitive personal data.

8. Confidentiality

8.1. The confidentiality of personal data must be respected by the Society when processing data at all times with access to the same limited on a need to know basis.

8.2. The Society shall maintain the confidentiality of the personal data throughout and even after the user is no longer of concern to the Society.

8.3. Health data will be kept separate from other personal data and will be accessible by healthcare providers or specific personnel employed to manage health data by the KRCS under confidentiality guarantees.

8.4. The data controller may specify other categories of personal data that will require additional safeguards and restrictions and may be classified as sensitive personal data.

8.5. In the processing of sensitive personal data the data controller will specify further grounds on which these categories will be processed with consideration of:
   a) the increased risk of significant harm that may be caused to the data subject by processing this category of personal data.
   b) the degree of confidentiality attached to the category of personal data.
   c) the level of protection afforded by provisions applicable to personal data.

8.6. The data controller shall process personal data of children in a manner that protects their rights and best interests.

8.7. The data controller will incorporate a process of obtaining parental consent and age verification in order to process personal data of children.

9. Security

9.1. The Society will ensure and implement a high level of data security that is appropriate to the risks presented by the nature and processing of personal data taking into account the level of technology available and existing security conditions as well as the costs of implementing additional security measures.

9.2. In order to ensure and respect confidentiality, personal data will be filed and stored in a way that is accessible only to authorized staff and transferred only through the use of protected means of communication.

9.3. In order to ensure the confidentiality of the personal data, the Society shall take appropriate technical and organizational data security measures.

9.4. The nature of risks will include but not be limited to risk of accidental or unlawful/illegitimate destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.

9.5. Access to personal data/content/knowledge shall be restricted to authorized personnel using it in the performance of their duties at the Society and as determined by appropriate authorization of both the staff or volunteers' supervisor and data subjects.

9.6. Personal data/content/knowledge may not be used by any employee or staff for purposes other than the business of the Society.

9.7. Staff and volunteers allowed access of personal data/content/knowledge of the Society shall sign a non-disclosure agreement banning them from using the content for business other than the Society's core mandate.

9.8. Private email accounts shall not be used to transfer Personal Data.

9.9. Information technology will be used to process, communicate and store society data and information which will be classified as Confidential Information (CI).

9.10. Data security measures will be routinely reviewed and upgraded as deemed appropriate to ensure the level of protection is commensurate to the degree of sensitivity applied to personal data and considering the possible development of new technology in enhancing data security.

10. Accountability

10.1. The Society will be responsible for compliance and will be required to demonstrate that appropriate measures have been employed within the organization to comply with the data protection guidelines.

10.2. The Society will implement data protection training programs for all staff.

10.3. The Society will bear the burden of proof to establish the data subjects' consent of the processing of their personal data for a specific purpose.

10.4. The Society will ensure that it is as easy to withdraw as it is to give consent.

11. Rights of data subjects

11.1. A data subject has a right to—

a) be informed of the use to which their personal data is to be put.
b) withdraw consent at any time.
c) access their personal data in custody of data controller or data processor.
d) object to the processing of all or part of their personal data.
e) correction of false, inaccurate or misleading data.
f) deletion of false or misleading data about them.
g) request for erasure of their personal data where it irrelevant, excessive or was obtained unlawfully.

12. Data collection

12.1. When collecting personal data from the user, the Society shall inform the user of the following in writing/orally and in a manner and language that is understandable to the user:

a) The specific purpose(s) for which the personal data or categories of personal data will be processed.
b) Whether such data will be transferred to third parties and the specific third parties.
c) The data subject's right to request access to their personal data, or correction or deletion of it.

d) How to lodge a complaint with the data controller.
e) The mandate and contact details of the data controller.

12.2. Where data is not collected directly from the data subject either orally or in writing, other means will be considered as far as is practicable such as radio communication, posters and flyers in an accessible location, online postings and any other appropriate method of transmission.

12.3. At the request of the data subject the data controller may restrict the processing of personal data where:

a) The accuracy of the data is contested by the data subject.
b) The data subject has objected to the processing.

13. Data Protection Impact Assessments

13.1. Where a type of processing in particular using new technology, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

13.2. A single assessment may address a set of similar processing operations that present similar high risks.

13.3. A data protection impact assessment shall in particular be required in the case of:

a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; or
b) a systematic monitoring of a publicly accessible area on a large scale.

13.4. The assessment shall contain at least:

a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
c) an assessment of the risks to the rights and freedoms of data subjects; and
d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Policy taking into account the rights and legitimate interests of data subjects and other persons concerned.

14. Data retention and disposal

14.1. Data will not be kept in a form that allows data subjects to be identified for longer than needed for the legitimate Society's purposes or other purposes for which the Society collected it.

14.2. The purposes of data retention shall include satisfying any legal, contractual, accounting or reporting requirements.

14.3. Personal data may be retained for a longer period in the event of a complaint there is reasonable belief that there is a prospect of litigation in respect to the Society's relationship with the data subject.

14.4. The Society shall take all reasonable steps to destroy or erase from its systems all personal data that are no longer required in accordance with the Society's Record Retention and Destruction Policy.

15. Transfer of personal data to third parties

15.1. The Society may transfer personal data to third parties with the data controller.

15.2. The Society may only transfer personal data/content/knowledge to third parties on condition that the third party affords a level of data protection the same or comparable to this Policy.

15.3. In order to mitigate risks associated with transfer of data to third parties, the Society will only transfer data to a third party if:

a) The data is stripped off personal and identifiable information;
b) The transfer is based on one or more legitimate basis including:
    i. explicit consent by the data subject;
    ii. compliance with national or international law; or
    iii. in exercise, establishment and defense of any contractual or legal obligations;
c) The personal data to be transferred is adequate, relevant, necessary and not excessive in relation to the purpose(s) for which it is being transferred;

d) The data subject has been informed either at the time of the collection or subsequently, about the potential transfer of his/her personal data;
e) The third party has in the past respected the confidentiality of personal data transferred to them by the Society; and
f) The third party maintains a high level of data security that protect personal data against the risk of accidental or unlawful/illegitimate destruction, loss, alteration unauthorized disclosure of, or access to it.

15.4. The Society will also ensure that transferring personal data does not negatively impact:
a) The safety and security of the Society staff, volunteers and beneficiaries.
b) The effective functioning of an operation or compromise in the Society's mission, vision or fundamental principles, for example due to the loss of trust and confidence between the Society and persons of concern.

15.5. The processing of sensitive personal data out of Kenya shall only be effected upon obtaining consent of a data subject and on obtaining confirmation of appropriate safeguards.

16. Data transfer records

16.1. The Society shall keep and maintain full and accurate records reflecting all phases of data management cycle, including records of data subjects' consents and procedures for obtaining consent, where consent is the legal basis of processing.

16.2. The data transfer records shall include, at a minimum:
a) the name and contact details of the individual entity authorizing the transfer;
b) clear descriptions of the personal data types;
c) data subject types;
d) processing activities;
e) processing purposes;
f) third-party recipients of the personal data;
g) personal data storage locations;
h) personal data transfers;
i) the personal data's retention period; and
j) a description of the security measures in place.

17. Data transfer agreements

17.1. The Society will require all third parties to comply with this Policy through an agreement or an MOU as part of the signing of partnership agreements. Such agreements will specify the specific purpose(s) and legitimate basis for the processing or transfer of personal data.

17.2. Data transfer agreements shall;
a) address the purpose(s) for data transfer, specific data elements to be transferred as well as data protection and data security measures to be put in place;
b) require the third party to undertake that its data protection and data security measures are in compliance with this Policy; and
c) stimulate consultation, supervision, accountability and review mechanisms for the oversight of the transfer for the life of the agreement.

17.3. The Legal Department of the Society shall review and approve all data transfer agreements and maintain copies of final agreements.

18. Data breach

18.1. The Society will maintain a register of all data breaches.

18.2. The Society's staff and volunteers will notify their line managers as soon as possible upon becoming aware of a personal data breach.

18.3. The member of staff or volunteer will record the breach.

18.4. If a personal data breach is likely to result in personal injury or harm to a data subject, the data controller will communicate the personal data breach to the data subject and take mitigating measures as appropriate without undue delay. In such cases, the data controller shall also notify the Secretary General of the personal data breach.

18.5. The notification will describe:

a) The nature of the personal data breach, including the categories and number of data subjects and data records concerned;
b) The known and foreseeable adverse consequences of personal data breach; and
c) The measures taken or proposed to be taken to mitigate and address the possible adverse impacts of the personal data breach.

19. External use and legal provisions

19.1. Title to all data belonging to the Society resulting from data processing shall reside in the Society and shall be protected by data protection laws of the Country.

19.2. Third parties may not process data belonging to the Society without consultation with the Society.

19.3. Any data processed jointly shall be jointly owned by the Society and third party with whom the joint processing was done.

19.4. Nothing in this policy will prevent legal action from being undertaken against a person who violates the provisions of this policy or of any Kenyan laws and regulations.

19.5. All matters arising out of or relating to this policy shall be governed by and are to be construed in accordance with the Laws of Kenya, excluding any conflict of law provisions, with Kenyan courts having exclusive jurisdiction in all disputes arising therein.

20. Periodic review of the knowledge management policy

20.1. This policy will be reviewed every three years or when need arises, whichever comes first.

Document management framework

Author Department	
Date Approved	
Name of Approver	
Proposed Revision Date	
Date of Revision	
Proposed Revision Date	