YOUTH FOR INTEGRITY BUILDING ORGANIZATION

DATA PROTECTION AND PRIVACY POLICY

Adapted from the Kenya Data Protection Policy

JULY 2023.

PREAMBLE

In today's digital age, the importance of protecting personal data cannot be overstated. We recognize that the trust and confidence you place in us when sharing your personal information is of utmost importance. At Youth For Integrity Building (YIB), we are committed to upholding the highest standards of data protection and privacy. Therefore, we have developed this policy to ensure that your data is handled with the utmost care, in compliance with applicable laws and regulations.

Our policy is built on the principles of transparency, consent, security, accuracy, and accountability. We strive to be transparent about our data practices, clearly explaining the purpose for which your data is collected and used. We obtain your informed consent before collecting any personal information and ensure that it is used only for the intended purposes. To protect your data, we have implemented robust security measures, including encryption, secure storage systems, and regular data backups. We also take steps to ensure the accuracy and integrity of your personal information, providing mechanisms for you to update or correct any inaccuracies.

We understand the importance of limiting data retention and controlling data sharing and disclosure. We do not sell, trade, or rent your personal information to third parties, and we only share it with trusted partners and service providers who assist us in carrying out our activities, and only to the extent necessary. We ensure that these third parties also have appropriate data protection measures in place. In the event of a data breach, we have procedures in place to promptly assess and mitigate the impact, and we will notify you and relevant authorities as required by law.

By adhering to these principles and objectives, we aim to build trust and confidence among our members, volunteers, and stakeholders in how we handle your personal data. We are committed to continuously improving our data protection practices and ensuring compliance with evolving data protection laws and regulations.

Thank you for your continued support and trust in Youth For Integrity Building. We encourage you to read our Data Protection and Privacy Policy in detail to understand how we protect your personal information. If you have any questions or concerns, please do not hesitate to reach out to us.

Executive Director,
Youth For Integrity Building (YIB).

TABLE OF CONTENT

1. INTRODUCTION

1.1. ***Youth For Integrity Building (YIB) Overview***: YIB is a community based organization established under the Community Groups Registration Act No. 30 of 2022.

1.2. ***YIB organization Mission:*** To empower young people with the knowledge, skills, and resources to become lead agents of change in promoting integrity, ethical leadership and social justice.

1.3. ***YIB organization vision***: To build a world in which all individuals and communities have the tools and resources they need to sustainably thrive, and where integrity, democracy, and social justice are valued and promoted.

1.4. YIB is fully committed to the principle of honesty, integrity and fair play in the delivery of services to the public. YIB is committed to complying with all relevant Kenyan legislation and applicable global legislations. YIB is also committed to protecting the privacy and data of its members, volunteers, and stakeholders.

2. PURPOSE

Recent concerns about the security of personal data stored in institutions have led to Governments enacting data protection regulations. In 2018 the European Union (EU) operationalized the General Data Protection Regulations (GDPR) that govern how companies handle personal data. Consequently, in 2019 Kenya enacted its own Data Protection Act. The regulations seek to protect the privacy of individuals by enforcing responsible processing of personal data. This includes embedding principles of lawful processing, minimizing the collection of data, ensuring the accuracy of data and adopting security safeguards to protect personal data. This policy,therefore, provides guidance on how YIB will handle the data it collects. It helps YIB comply with the data protection law, protect the rights of the data subjects and protects YIB from risks related to breaches of data protection

3. SCOPE

The policy applies to:
a) YIB employees, volunteers, and all YIB's stakeholders such as Trustees, implementing partners, vendors, contractors and any other third party who handle and use YIB information (where YIB is the ***'Controller'*** for the personal data being processed, be it in manual and automated forms or if others hold it on their systems for YIB).
b) All personal data processing YIB carries out for others (where YIB is the ***'Processor'*** for the personal data being processed) .
c) All formats, e.g., printed and digital information, text and images, documents and records, data and audio recordings.

5. DEFINITION OF TERMS

a. ***Data controller:*** A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of the processing of personal data.
b. ***Data processor:*** A natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.

c. ***Data subject:*** An identified or identifiable natural person who is the subject of personal data.
d. ***Personal data :*** Any information relating to an identified or identifiable natural person.
e. ***A 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.
f. ***Sensitive personal data:*** Data that reveals the natural person's race, health status, ethnic, social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses sex, or the sexual orientation of the data subject.
g. ***Processing data:*** Any operation or sets of operations performed on 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.

6. OBJECTIVES OF THIS POLICY.

6.1. To safeguard the personal data of our employees, volunteers, and stakeholders from unauthorized access, disclosure, alteration, or destruction.

6.2. To ensure compliance with applicable data protection laws and regulations, including the General Data Protection Regulation (GDPR) and other relevant legislation in our jurisdiction.

6.3. To build trust and confidence among our employees, volunteers, and stakeholders in how we handle their personal data.

6.4. To be transparent about our data practices and provide clear information to individuals regarding the collection, use, and sharing of their personal data.

6.5. To obtain informed consent from individuals before collecting their personal data, and to clearly explain the purpose for which the data will be used.

6.6. To take reasonable steps to ensure that personal data is accurate, complete, and up-to-date, and to provide mechanisms for individuals to update or correct their personal information.

6.7. To retain personal data only for as long as necessary to fulfill the purposes for which it was collected, or as required by law, and to securely dispose of it once it is no longer needed.

6.8. To ensure that personal data is shared with trusted partners and service providers only to the extent necessary, and to have appropriate data protection measures in place with these third parties.

6.9. To not knowingly collect personal information from children under the age of 18 without parental/guardian consent, and to delete such information if inadvertently collected.

6.10. To have procedures in place to promptly assess and mitigate the impact of any data breaches, and to notify affected individuals and relevant authorities as required by law.

7. POLICY STATEMENT

YIB recognizes that the protection of individuals through lawful, legitimate, and responsible processing and use of their personal data is a fundamental human right. YIB will ensure that it protects the rights of data subjects and that the data it collects, and processes is done in line with the required legislation. YIB staff must comply with this policy, breach of which could result in disciplinary action.

8. PRINCIPLES.

8.1. We collect only the necessary personal information required to carry out our activities and services. We obtain consent from individuals before collecting their data and clearly explain the purpose for which the data will be used.

8.2. We implement appropriate security measures to protect personal data from unauthorized access, disclosure, alteration, or destruction. This includes encryption, secure storage systems, and regular data backups.

8.3. We retain personal data only for as long as necessary to fulfill the purposes for which it was collected, or as required by law. Once the data is no longer needed, we securely dispose of it.

8.4. We do not sell, trade, or rent personal data to third parties. We only share personal data with trusted partners and service providers who assist us in carrying out our activities, and only to the extent necessary. We ensure that these third parties also have appropriate data protection measures in place.

8.5. We strive to be transparent about our data practices and provide individuals with access to their personal data. Upon request, individuals can review, update, or delete their personal information, subject to legal limitations.

8.6. We take reasonable steps to ensure that personal data is accurate, complete, and up-to-date. Individuals have the right to request corrections to their personal information if they believe it is inaccurate or incomplete.

8.7. We do not knowingly collect personal information from children under the age of 18 without parental/guardian consent. If we become aware that we have inadvertently collected personal data from a child, we will delete it as soon as possible.

8.8. We comply with applicable data protection laws and regulations, including the General Data Protection Regulation (GDPR) and other relevant legislation in our jurisdiction.

8.9. In the event of a data breach, we have procedures in place to promptly assess and mitigate the impact. We will notify affected individuals and relevant authorities as required by law.

8.10. We provide regular privacy awareness and training to our employees and volunteers to ensure they understand their responsibilities in safeguarding personal data.

9. ROLES AND RESPONSIBILITIES.

All employees, volunteers and other stakeholders must:

a) Read, understand and comply with the contents of this policy

b) Report suspicions of breaches promptly

All project leads and managers must

a) Ensure employees, volunteers and other stakeholders they work with are aware of the contents of this policy

b) Conduct risk assessments, and update controls and procedures to mitigate the risk of data breaches

The Executive Director, Operations Manager, Programmes manager and H.R Manager are responsible for ensuring employees, volunteers and stakeholders are aware of the policy and are supported to implement and work by it, as well as creating a management culture that encourages a focus on data protection.

10. DUTY TO NOTIFY

YIB has a duty to notify data subjects of their rights before processing data. YIB will therefore inform the data subjects of their right:

a) To be informed of the use to which their personal data is to be put.

b) To access their personal data in YIB's custody.

c) To object to the processing of all or part of their personal data.

d) To the correction of false or misleading data.

e) To deletion of false or misleading data about them.

11. LAWFUL AND FAIR PROCESSING OF DATA

YIB will only process data where they have a lawful basis to do so. Processing personal data will only be lawful where the data subject has given their consent for one or more specific purposes or where the processing is deemed necessary:

a) For the performance of a contract to which the data subject is a party (for instance a contract of employment).

b) To comply with the YIB's legal obligations.

c) To perform tasks carried out in the public interest or the exercise of official authority.

d) To protect the vital interests of the data subject or another person.

e) To pursue YIB's legitimate interests where those interests are not outweighed by the interests and rights of data subjects.

f) For historical, statistical, journalistic, literature and art or scientific research.

12. MINIMIZATION OF COLLECTION

12.1. YIB will not process any personal data for a purpose for which it did not obtain consent. Should such a need arise, then consent must be obtained from the data subject.

12.2. YIB will collect and process data that is adequate, relevant, and limited to what is necessary.

12.3. YIB employees must not access data which they are not authorized to access nor have a reason to access.

12.4. Data must only be collected for the performance of duties and tasks; employees must not ask data subjects to provide personal data unless that is strictly necessary for the intended purpose.

12.5. Employees must ensure that they delete, destroy, or anonymize any personal data that is no longer needed for the specific purpose for which they were collected.

13. ACCURACY OF DATA

YIB must ensure that the personal data it collects and processes is accurate, kept up to date, corrected or deleted without delay. All relevant records must be updated should employee be notified of inaccuracies. Inaccurate or out of date records must be deleted or destroyed.

14. SAFEGUARDS AND SECURITY OF DATA

YIB has instituted data security measures which are laid out in the Information security policy and procedures. These measures serve to safeguard personal data and must be complied with accordingly.

15. CONSENT

Where necessary, YIB will maintain adequate records to show that consent was obtained before personal processing data. Data will not be processed after the withdrawal of consent by a data subject.

16. PROCESSING DATA RELATING TO A CHILD

YIB will not process data relating to a child unless consent is given by the child's guardian or parent and the processing is in such a manner that protects and advances the rights and best interests of the child in line with YIB Safeguarding policy. YIB will institute adequate mechanisms to verify the age and obtain consent before processing the data.

17. DATA PROTECTION IMPACT ASSESSMENT

YIB will undertake a data protection impact assessment whenever they identify that the processing operation will likely result in a high risk to the rights and freedoms of any data subject. The data protection impact assessment will be done before processing the data.

18. PROCESSING SENSITIVE PERSONAL DATA

YIB will process sensitive personal data only when:

a) The processing is carried out in the course of legitimate activities with appropriate safeguards and that the processing relates solely to the staff or to persons who have regular contact with YIB, and the personal data is not disclosed outside that YIB without the consent of the data subject.

b) The processing relates to personal data that has been made public by the data subject.

c) Processing is necessary for:

i. The establishment, exercise or defence of a legal claim.

ii. The purpose of carrying out the obligations and exercising specific rights of the controller or of the data subject.

iii. Protecting the vital interests of the data subject or another person where the data subject is physically or legally incapable of giving consent.

19. TRANSFERRING PERSONAL DATA OUT OF KENYA

YIB will transfer personal data out of Kenya only when they have:

a) Proof of appropriate measures for security and protection of the personal data, and the proof provided to the Data Protection Commissioner in accordance with Kenya's Data Protection Act, 2019, such measures include that data is transferred to jurisdictions with commensurate data protection laws.

b) The transfer is necessary for the performance of a contract, implementation of per-contractual measures such as:

i. For the conclusion or performance of a contract to which the data subject is part of.

ii. For matters of public interest.

iii. For legal claims.

iv. To protect the vital interests of data subjects.

v. For compelling legitimate interests pursued by the data controller or data processor which are not overridden by the interests, rights and freedoms of the data subjects.

YIB will process sensitive personal data out of Kenya only after obtaining the consent of a data subject and on receiving confirmation of appropriate safeguards.

20. ONWARD REPORTING

In line with regulatory requirements, YIB will report to the Data Protection Commissioner any data breach within 72 hours of being aware. YIB will also communicate the data breach to the data subject as soon as is practical unless the identity of the data subject cannot be established.

21. TRAINING AND AWARENESS

YIB will train staff on the contents and implementation of this policy. Staff who join YIB will be required to go through an induction process that entails familiarization with this policy. YIB will ensure that the requirements of this policy form part of its agreement with its grantees, contractors and third parties who process YIB's data.

22. GRANTEES OR PARTNERS

Grantees and partners of YIB must report breaches of YIB's data in their custody within 48 hours using the emails provided above. Grantees and partners must also abide by this policy and institute adequate mechanisms to safeguard the privacy of individuals data.

23. INDEPENDENT ASSURANCE

The adequacy and effectiveness of YIB's data protection procedures is subject to the regular internal audit reviews where necessary YIB may call an external review provide assurance over the integrity.

24. DATA RETENTION

The Data retention period in YIB is determined by legitimate needs. Adequate records of decision making will be maintained to show cause.

25. REVIEW OF THIS POLICY

The Operations Manager and the Programmes Manager are responsible for ensuring that this policy is reviewed on a timely basis. This policy will be reviewed after every two years.

26. RELATED POLICIES

This policy should be read in conjunction with:

a) YIB Code of conduct

b) Misconduct, disciplinary and grievance policy

c) Information security policy

d) Consent and Consent Management Procedures

Youth For Integrity Building Organization (YIB).

P.O Box 921-80108, Kilifi, Kenya.

Telephone No: +254 710785237.

Email: info@yc4integritybuilding.org