



NANDI COUNTY YOUTH BUNGE ASSOCIATION

Data Protection and Privacy Policy 2026

In collaboration with the Open Institute

DATE

October 2026

ORGANISATION

NCYBA

ADDRESS

P.O. Box 600-30300 Kapsabet

Table of Contents

ACRONYMS/LIST OF ABBREVIATIONS	6
FOREWORD	7
ACKNOWLEDGMENTS	9
PREAMBLE	10
1. PURPOSE OF THE POLICY	11
2. POLICY OBJECTIVES	11
3. DEFINITIONS AND INTERPRETATION	12
4. DATA GOVERNANCE PRINCIPLES	15
5. DATA COLLECTION STANDARDS	17
5.3 Prohibited Collection Practices	17
6. PERSONAL AND SENSITIVE DATA	18
7. DATA RELATING TO MINORS	20
7.1 Data Collection	20
7.2 Consent and Authorization	20
7.3 Photography and Media Use	20
7.4 Secure processing	21
8. MEMBERSHIP AND YOUTH DATABASE MANAGEMENT	22
8.1 Institutional Ownership	22
8.2 Purpose of Membership Data	22
8.3 Prohibited Uses of Membership Data	22
8.4 Authorized Access and Exports	23
8.5 Access Termination	23
9. DATA USE FOR RESEARCH, ADVOCACY, AND PUBLIC PARTICIPATION	24
9.1 Permitted Activities	24
9.2 Research Ethics and Safeguards	24
9.3 Anonymisation and Aggregation	24
9.4 Responsible Presentation	25
10. PHOTOGRAPHS, VIDEOS, AUDIO, AND TESTIMONIALS	26
10.1 General Principles	26
10.2 Consent Requirements	26
10.3 Event Notices	26
10.4 Withdrawal and Deletion	26
10.5 Contextual Misuse	27
11. DATA ACCESS AND ROLE-BASED PERMISSIONS	28
11.1 Principle of Least Privilege	28
11.2 Access Categories	28
11.3 User Account Management	28

11.4 Immediate Revocation	29
12. DATA SECURITY AND INFORMATION SECURITY	30
12.1 Digital Security	30
12.2 Physical Security	30
12.3 Mobile Devices	31
12.4 Communication Platforms	31
13. DATA SHARING AND THIRD-PARTY MANAGEMENT	32
13.1 General Principles	32
13.2 Categories of Third Parties	32
13.3 Safeguards for Data Sharing	32
13.4 Data Processing Agreements	33
14 CROSS-BORDER DATA TRANSFERS	34
14.1 Applicability	34
14.2 Legal and Institutional Safeguards	34
14.3 Cloud and Technology Services	35
15. DATA RETENTION AND DISPOSAL	36
15.1 Data Lifecycle Approach	36
15.2 Retention Schedule	36
15.3 Periodic Review	36
15.4 Secure Disposal	37
15.5 Disposal Log	37
16. DATA SUBJECT RIGHTS	38
16.1 Rights of Data Subjects	38
16.2 Exercising Rights	38
16.3 Requests Relating to Children	39
17. DATA BREACH AND INCIDENT MANAGEMENT	39
17.1 Definition and Examples	39
17.2 Breach Response Process	39
17.3 Documentation	40
18. GOVERNANCE STRUCTURE AND RESPONSIBILITIES	42
18.1 Governing Board	42
18.2 Executive Leadership	42
18.3 Data Protection Officer or Designated Data Protection Lead	42
18.4 Programme and Project Managers	43
18.5 ICT or Systems Administrators	43
18.6 Staff and Volunteers	43
18.7 Third Parties	44
19. DATA PROTECTION IMPACT AND RISK ASSESSMENTS	45
19.1 When to Conduct an Internal and External Assessment	45
19.2 Assessment Content	45

20. DATA ETHICS AND RESPONSIBLE USE	46
20.1 Ethical Framework	46
20.2 Ethical Decision-Making	46
21.3 Prohibited Data Practices	47
The following practices are strictly prohibited:	47
21. TRAINING AND ORGANISATIONAL CAPACITY	48
21.1 Training Requirements	48
21.2 Training Records	48
21.3 Capacity Building	48
22. COMPLIANCE, MONITORING, AND AUDIT	49
22.1 Periodic Compliance Reviews	49
22.2 Access Audits	49
22.3 Database Reviews	49
22.4 Security Assessments	49
22.5 Partner Compliance Reviews	49
22.6 Internal Reporting	49
22.7 Corrective Action	50
23. POLICY VIOLATIONS AND DISCIPLINARY ACTION	51
23.1 Proportionality	51
23.2 Range of Responses	51
23.3 Whistleblower Protection	51
24. COMPLAINTS AND REPORTING CHANNELS	52
24.1 Privacy Concerns and Complaints	52
24.2 Reporting Data Security Incidents	52
24.3 Anonymous Reporting	52
24.4 Response to Complaints	52
25. REVIEW AND AMENDMENT OF THE POLICY	53
25.1 Regular Review	53
25.2 Triggered Review	53
25.3 Amendment Process	53
26. RELATED DOCUMENTS	54
ANNEX TEMPLATES FOR NCYBA DATA PROTECTION POLICY	55
ANNEX A: DATA INVENTORY & PROCESSING REGISTER TEMPLATE	55
ANNEX B1: STANDARD CONSENT FORM TEMPLATE	56
NCYBA DATA PROCESSING CONSENT FORM: For Participants Aged 18+	56
ANNEX B2: PARENTAL/GUARDIAN CONSENT FORM TEMPLATE	58
NCYBA MINOR DATA PROCESSING CONSENT FORM: For Participants Under 18 Years	58
ANNEX B3: MULTIMEDIA CONSENT & RELEASE FORM	60
NCYBA PHOTO/VIDEO/AUDIO CONSENT FORM	60
ANNEX C: DATA RETENTION SCHEDULE TEMPLATE	62



ANNEX D: LEGITIMATE INTERESTS ASSESSMENT (LIA) TEMPLATE	64
ANNEX E: DATA SUBJECT REQUEST FORM	66
ANNEX F: DATA BREACH RESPONSE PLAN & FORM	68
ANNEX G: DATA PROCESSING AGREEMENT TEMPLATE	70
ANNEX H: STAFF/VOLUNTEER CONFIDENTIALITY UNDERTAKING	72
ANNEX I: PRIVACY NOTICE TEMPLATE	73

ACRONYMS/LIST OF ABBREVIATIONS

DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
MFA	Multi-factor Authentication
ICT	Information, Communication Technology
KNCCI	Kenya National Chamber of Commerce and Industry
MEAL/MEL	Monitoring, Evaluation, Accountability, and Learning
NCYBA	Nandi County Youth Bunge Association

FOREWORD

Awareness is not enough. This has been the central lesson of Open Institute's work on data protection over the past year. Through the Ficha Uchi campaign <https://fichauchi.org/>, we reached 557,674 people online between June and September 2026, bringing the campaign's five-year reach to more than 14.7 million. Among exposed audiences, support for Kenya's Data Protection Act increased by 6 percentage points. Yet our engagement with communities revealed a significant gap between awareness and the capacity to act. In a baseline survey of 359 Kilifi residents, only 41% understood what personal data is, 9% knew how to report a scam, and just 13% had heard of the Office of the Data Protection Commissioner. Similarly, among 55 school leaders surveyed before our data protection training for teachers, two-thirds reported having experienced data misuse, but only 30% knew what action to take.

At the institutional level, our pilot Data Protection Impact Assessment with a county government similarly highlighted the implementation challenge: sensitive records were being managed through physical files and flash disks, without a designated data protection officer or standard privacy notices. In March 2026, the second East Africa Data Governance Conference also arrived at a similar conclusion at regional level: the region has laws and frameworks, but its central challenge is implementation. These findings demonstrate that effective data protection requires more than awareness, it requires practical systems, knowledge and accountability. Our interventions have shown that this transition is possible. Following offline data protection sessions in Mombasa and Kwale, support for the Data Protection Act increased from 50% to 77%. Those intending to verify information before sharing it rose from 50% to 83%, while those indicating they would report a scam increased from 59% to 83%.

It is against this background that I welcome the Nandi County Youth Bunge Association's (NCYBA) Data Protection and Privacy Policy. The policy is an important example of turning legal principles into practical organisational safeguards. It establishes clear requirements for data collection, consent, storage, retention and disposal; protects the data of minors through parental or guardian consent; provides individuals with rights to access, correct and delete their information; and sets clear responsibilities for staff, volunteers, data protection officers and third-party partners. It also provides for breach management, including notification to the Data Commissioner within 72 hours, and establishes safeguards for sharing data outside Kenya. Importantly, the policy was developed through

a consultative process, giving those responsible for implementing it an opportunity to shape the systems they will use.

This is more than a policy document; it is a milestone in moving from awareness to practice. Its success will ultimately be measured by whether NCYBA members understand and apply it, whether data registers remain current, whether people's rights are respected, and whether the organisation can respond effectively when things go wrong. It also provides a practical model that other civil society organisations can learn from and adapt.

Open Institute is proud to have supported NCYBA in this journey and remains committed to strengthening responsible data stewardship across Kenya. We are looking forward to working with CSOs and CBOs in other counties and sectors to develop, adapt and institutionalise similar data protection policies and practical systems that protect people's rights and build trust in the organisations that serve them. We hope the NCYBA experience will inspire many more organisations to take this important step from knowing the law to putting it into practice.

Congratulations

Christine Ajulu

Deputy Executive Director, Open Institute
October 2026

ACKNOWLEDGMENTS

The Nandi County Youth Bunge Association (NCYBA) extends its sincere gratitude to all those whose contribution made the development of this Data Protection and Privacy Policy possible.

We acknowledge, with appreciation, the County Government of Nandi, through the Office of the County Secretary, for its support and engagement throughout the development of this Policy. We further acknowledge the County Assembly of Nandi, through the Office of the Clerk, for its guidance and cooperation in aligning this Policy with the county's broader governance and legislative framework.

We extend our appreciation to the Open Institute for the technical support extended to this process, which was instrumental in shaping the policy's technical and data governance standards. Our gratitude goes to the members of the Nandi County Youth Bunge Association, whose participation, feedback and lived experience grounded this Policy in the realities it seeks to address.

We also acknowledge the Nandi County Civil Society Organizations, the Kenya National Chamber of Commerce and Industry (KNCCI) – Nandi Chapter, and the Nandi County media fraternity, for their engagement, insight and support throughout this process.

This Policy is the product of a collective effort, and NCYBA remains grateful to every individual and institution who contributed to its development.

PREAMBLE

Nandi County Youth Bunge Association (NCYBA) is a youth-led membership organization committed to empowering young people through leadership development, civic engagement, public participation, governance accountability, research, advocacy, and community mobilization. In pursuing this mission, NCYBA collects, processes, stores, and shares information about its members, staff, volunteers, programme participants, partners, donors, and the communities it serves.

NCYBA recognizes that data is simultaneously an institutional asset, a source of public trust, and a potential source of harm if poorly governed. Young people, community members, and partners entrust NCYBA with their personal information in the expectation that it will be handled responsibly, ethically, and securely. The misuse, loss, or unauthorized disclosure of this information can cause harm to individuals, undermine and erode community confidence and trust, expose the organization to legal liability, and compromise the safety of vulnerable youth.

This policy affirms NCYBA's commitment to responsible data governance. It establishes the principles, standards, and accountability mechanisms through which NCYBA will collect, use, store, share, and dispose of personal data. It applies to all institutional activities, whether conducted digitally or physically, and binds everyone who acts on behalf of NCYBA.

This policy is not merely a legal compliance document. It is an operational governance instrument designed to protect the dignity, privacy, and rights of every individual whose data NCYBA processes, while enabling the organization to fulfil its mission effectively and accountably.

1. PURPOSE OF THE POLICY

The purpose of this policy is to:

1. Protect the privacy and personal data rights of all individuals who interact with NCYBA, including members, participants, staff, volunteers, donors, and community members;
2. Establish a framework for lawful, fair, and transparent data processing in accordance with the Data Protection Act, 2019 of Kenya and applicable regulatory guidance;
3. Define institutional accountability for data governance, assigning clear responsibilities to the Board, management, staff, volunteers, and third parties;
4. Reduce data-related risks, including unauthorized access, accidental disclosure, data misuse of whatever nature, and loss of institutional trust;
5. Protect youth and community members, particularly children and vulnerable individuals, from harm arising from improper data handling;
6. Enable the responsible use and re-use of data for programme delivery, research, monitoring and evaluation, advocacy, public participation, and organizational management;
7. Provide a basis for compliance, partnership accountability, and institutional credibility; and
8. Foster a culture of responsible data use throughout NCYBA operations.

2. POLICY OBJECTIVES

This policy seeks to achieve the following objectives:

- Establish clear principles for lawful, fair, and responsible data processing across all NCYBA activities;
- Protect the rights, privacy, and dignity of data subjects, particularly young people and marginalized community members;
- Define the roles, responsibilities, and accountability structures for data governance within NCYBA;
- Prevent the misuse of membership and youth databases for unauthorized political, commercial, or personal purposes.

3. DEFINITIONS AND INTERPRETATION

In this policy, unless the context otherwise requires:

"Anonymisation" means the process of removing or modifying personal identifiers so that data can no longer be linked to a specific individual, and the process is irreversible.

"Consent" means any freely given, specific, informed, and unambiguous indication of a data subject's wishes by which they signify agreement to the processing of their personal data.

"Cross-border data transfer" means the transfer of personal data from Kenya to another country or international organization.

"Data breach" means 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.

"Data controller" means NCYBA as the natural or legal person that, alone or jointly with others, determines the purposes and means of processing personal data.

"Data minimisation" means the principle that personal data collected should be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

"Data processor" means a natural or legal person, public authority, agency, or other body that processes personal data on behalf of NCYBA.

"Data protection impact assessment (DPIA)" means a systematic evaluation of the potential impact of a processing activity on the privacy and rights of data subjects.

"Data subject" means an identified or identifiable natural person whose personal data is processed by NCYBA.

"Disposal" means the secure and irreversible destruction of personal data when it is no longer required.

"Encryption" means the process of converting data into a coded form to prevent unauthorized access.

"Legitimate interests" means the lawful interests of NCYBA in processing data, provided that such interests do not override the fundamental rights and freedoms of the data subject.

"Multi-factor authentication (MFA)" means a security mechanism requiring two or more verification methods to access a system or account.

"Personal data" means any information relating to an identified or identifiable natural person, including but not limited to name, identification number, location data, online identifier, or factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.

"Processing" means any operation or set of operations performed on personal data, whether or not by automated means, including

- (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.

"Pseudonymisation" means the processing of personal data in such a manner that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and subject to technical and organizational measures to ensure non-attribution.

"Retention" means the period during which personal data is kept by NCYBA before secure disposal.

"Sensitive personal data" means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, or data concerning a natural person's sex life or sexual orientation, as well as personal data relating to children.

"Third party" means any natural or legal person, public authority, agency, or body other than the data subject, NCYBA, or a data processor authorized by NCYBA.

"Audit rights" means the contractual right reserved by NCYBA to verify a third party's or processor's compliance with its data protection obligations, including through the provision of information, documentary review, or inspection on reasonable notice

"Confidentiality obligation" means the binding commitment, preferably recorded in writing through a Data Processing Agreement, by which a third party or processor undertakes not to disclose personal data shared with it by NCYBA and to restrict access to it to named persons who require it.

"Data" means any information processed by NCYBA in connection with its mandate, whether or not it constitutes personal data.

"Necessary data" (used interchangeably with "minimum necessary data") means the specific data elements that are adequate, relevant, and limited to what is required to achieve a defined and lawful purpose, applying the principle of data minimisation

"Return or deletion of data" means the obligation on a third party, processor, departing staff member, volunteer, or other person holding NCYBA data, upon termination of the relevant relationship or completion of the purpose for which the data was shared, to return all such data to NCYBA or to permanently and irreversibly delete every copy in its possession or control, including backups and derived datasets.

4. DATA GOVERNANCE PRINCIPLES

NCYBA processes all personal data in accordance with the following principles:

4.1 Lawfulness, Fairness, and Transparency

Personal data shall be processed lawfully, fairly, and in a transparent manner. NCYBA shall inform data subjects about how their data is collected, used, stored, and shared through clear privacy notices and collection statements. NCYBA shall not process data in ways that are deceptive, misleading, or contrary to the reasonable expectations of the data subject.

4.2 Purpose Limitation

Personal data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes. NCYBA shall not use data collected for one purpose for an unrelated purpose without a fresh lawful basis and, where required, fresh consent.

4.3 Data Minimisation

NCYBA shall collect only the personal data that is adequate, relevant, and necessary for the specific purpose identified. The organization shall not collect personal information simply because it may be useful in the future. Programme staff and researchers shall justify the data elements they collect and shall review data collection instruments regularly to eliminate unnecessary fields.

4.4 Data Accuracy

Personal data shall be accurate and, where necessary, kept up to date. NCYBA shall take reasonable steps to ensure that inaccurate personal data is erased or rectified without delay. Data subjects shall be encouraged to update their information, and programme teams shall verify critical data at reasonable intervals.

4.5 Storage Limitation

Personal data shall be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed. NCYBA shall establish and adhere to a Data Retention Schedule that defines retention periods for each category of data.

4.6 Integrity and Confidentiality

Personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical and organizational measures. Access to data shall be granted on a need-to-know basis.

4.7 Accountability

NCYBA, as the data controller, is responsible for and must be able to demonstrate compliance with these principles. The Board, Executive Leadership, and the Data Protection Officer shall maintain records of processing activities, conduct periodic audits, and ensure that staff and partners are held accountable for compliance.

4.8 Privacy and Data Protection by Design

NCYBA shall integrate data protection considerations into the design of its programmes, databases, research methodologies, digital platforms, and partnerships from the outset. New systems, tools, or activities involving personal data shall be assessed for privacy implications before implementation.

4.9 Responsible and Ethical Data Use

Beyond legal compliance, NCYBA commits to using data in ways that respect human dignity, avoid discrimination, prevent harm, and maintain community trust. The fact that data can legally or technically be collected does not automatically mean that NCYBA should collect it. Ethical judgment shall guide all data processing decisions.

5. DATA COLLECTION STANDARDS

5.1 Necessity and Proportionality

NCYBA shall collect personal data only where:

- (a) The collection is necessary for a clearly defined and legitimate institutional purpose;
- (b) The data elements are relevant and proportionate to that purpose;
- (c) Less intrusive means of achieving the purpose have been considered; and
- (d) The collection is authorized by this policy or a specific programme protocol.

5.2 Collection Instruments and Notices

All data collection shall be accompanied by appropriate notices or consent mechanisms, including:

- (a) Data collection notices: Clear statements provided at the point of collection explaining who NCYBA is, what data is being collected, why, how long it will be kept, who it may be shared with, and how individuals can exercise their rights;
- (b) Consent forms: Standardized forms for activities requiring consent, adapted to the context (adult participants, minors, multimedia);
- (c) Surveys and research instruments: Tools reviewed and approved by programme managers to ensure data minimization and ethical compliance;
- (d) Registration forms: Physical or digital forms for events, trainings, and programmes;
- (e) Digital forms: Online forms hosted on approved platforms with appropriate security configurations; and
- (f) Membership forms: Forms capturing information necessary for membership administration, governance, and communication.

5.3 Prohibited Collection Practices

The following collection practices are prohibited:

- (a) Collecting personal data without a defined purpose or lawful basis;
- (b) Collecting excessive or irrelevant data because it "might be useful later";
- (c) Collecting sensitive personal data without heightened justification and safeguards;
- (d) Using deception or misrepresentation to obtain personal data;
- (e) Collecting data from third parties without confirming that the third party had authority to share it and that NCYBA has a lawful basis to process it; and
- (f) Covert surveillance or recording without legal authority and, where required, consent

6. PERSONAL AND SENSITIVE DATA

6.1 Enhanced Protection

Sensitive personal data, as defined in Section 3 of this policy, shall be subject to enhanced protection. NCYBA shall process sensitive personal data only where:

- (a) Processing is necessary and proportionate to a compelling institutional purpose;
- (b) A specific lawful basis applies, including explicit consent where required by law;
- (c) The data subject has been informed of the sensitive nature of the data and the specific protections in place;
- (d) Access is restricted to personnel with a strict need to know;
- (e) Enhanced security measures, including encryption where feasible, are applied; and
- (f) Individual-level personal data shall not be published in public reports, policy briefs, or media materials without explicit consent;

6.2 Categories Requiring Special Attention

The following categories of sensitive data require particular care:

- (a) **Health-related information:** Medical conditions, allergies, mental health information, disability status, and treatment records. Such data shall be collected only where necessary for participant safety or programme adaptation, stored separately from general records where practicable, and shared only with authorized personnel;
- (b) **Biometric information:** Fingerprints, facial recognition data, or other biometric identifiers. Collection of biometric data shall require explicit justification, enhanced security, and shall not proceed without a Data Protection Impact Assessment;
- (c) **Financial information:** Bank account details, mobile money identifiers, and payment card information. Such data shall be processed only for legitimate financial transactions, stored securely, and never shared for marketing or unrelated purposes;
- (d) **Identity documents:** National ID numbers, passport numbers, and birth certificates. These shall be collected only where legally required or operationally essential, and copies shall be stored securely with restricted access;
- (e) **Political opinions and affiliations:** Given NCYBA's civic engagement work, data about political opinions shall be handled with particular care to prevent targeting, discrimination, or unauthorized disclosure; and



- (f) **Information exposing vulnerability:** Data that could expose a person to stigma, discrimination, harm, or political targeting, including information about ethnicity, religion, sexual orientation, or economic status.

7. DATA RELATING TO MINORS

NCYBA works extensively with young people, including individuals under the age of 18. The protection of children's data is integral to NCYBA's child safeguarding commitment. All processing of children's personal data shall comply with this policy, the Data Protection Act, 2019, the Children's Act, and applicable child protection standards.

NCYBA and all its associates will adhere to the following when collecting and processing data relating to minors:

7.1 Data Collection

- (a) Data collection from children shall be limited to what is necessary for their safe participation in NCYBA activities;
- (b) Programme staff shall verify the age of participants where age determines consent requirements or safeguarding protocols;
- (c) Data collection from very young children (under 13) shall be avoided unless essential and authorized by a programme manager with appropriate safeguards.

7.2 Consent and Authorization

- (a) For children under 18, verifiable parental or guardian consent shall be obtained before processing personal data, except where processing is manifestly in the child's best interests and consent is not reasonably obtainable;
- (b) Consent forms for minors shall be separate from adult forms and shall clearly identify the parent or guardian providing consent, their relationship to the child, and their contact details;
- (c) Where a child is sufficiently mature to understand the implications of data processing, their assent shall be sought in addition to parental consent;
- (d) Health data and sensitive data relating to children shall require explicit parental consent and enhanced security.

7.3 Photography and Media Use

- (a) Photographs, videos, or audio recordings of children shall not be captured, published, or shared without specific parental or guardian consent obtained through the Multimedia Consent Form;
- (b) Even with consent, NCYBA shall avoid publishing identifying information alongside images of children, including full names, schools, addresses, or detailed locations;

- (c) Children in vulnerable situations shall not be photographed or filmed without exceptional justification and approval by the Executive Leadership.

7.4 Secure processing

- (a) Education records, health information, and vulnerability assessments relating to children shall be stored separately from general programme data where practicable;
- (b) Access to children's data shall be limited to designated programme staff and safeguarding officers;
- (c) Any disclosure of children's data to external parties, including government agencies, shall require authorization by the Executive Leadership and shall be documented.

8. MEMBERSHIP AND YOUTH DATABASE MANAGEMENT

8.1 Institutional Ownership

NCYBA membership databases, youth contact lists, and related records are institutional assets held in trust for the organization. They are not the personal property of any staff member, volunteer, board member, or office holder. All membership data shall be stored on approved institutional systems and shall not be downloaded, copied, or maintained on personal devices or accounts without explicit authorization.

8.2 Purpose of Membership Data

Membership data shall be used exclusively for:

- (a) Official NCYBA governance, communication, and programme administration;
- (b) Membership verification and electoral processes conducted under NCYBA's constitution and bylaws;
- (c) Organizing legitimate NCYBA activities, trainings, and events;
- (d) Fulfilling legal and regulatory obligations; and (e) Other purposes expressly authorized by the Board.

8.3 Prohibited Uses of Membership Data

The following uses of NCYBA membership and youth databases are strictly prohibited:

1. Political mobilization, campaigning, or advocacy for any candidate, party, or political cause without express Board authorization;
2. Commercial marketing, advertising, or sale of products or services;
3. Personal campaigning or promotion of individual interests unrelated to NCYBA's mission;
4. Sharing membership lists with political actors, candidates, or parties;
5. Unauthorized fundraising for personal or external causes;
6. Sale, transfer, or barter of membership information to any third party;
7. Bulk downloads or exports of membership data without authorization from the Executive Leadership or designated Data Protection Officer; and
8. Use of membership contact information to create parallel communication channels, WhatsApp groups, or mailing lists without institutional oversight.



8.4 Authorized Access and Exports

- 1) Access to membership databases shall be granted on a role basis;
- 2) Bulk exports, downloads, or reports containing personal data shall require authorization from the Executive Leadership or Data Protection Officer and shall be documented;
- 3) Staff and volunteers shall use institutional systems (e.g., approved databases, email systems) for membership communication. Personal email accounts, WhatsApp, or informal channels shall not be used to distribute membership lists or contact information;
- 4) Database administrators shall maintain logs of access, exports, and modifications where technically feasible.

8.5 Access Termination

- (a) When a staff member, volunteer, or board member exits their role or leaves NCYBA, their access to membership databases and related systems shall be revoked immediately or within 24 hours of exit;
- (b) Departing personnel shall return or delete all NCYBA data from personal devices and accounts, and shall sign a confirmation to this effect where required;
- (c) Former members of the organization shall not retain access to institutional databases or contact lists.



9. DATA USE FOR RESEARCH, ADVOCACY, AND PUBLIC PARTICIPATION

9.1 Permitted Activities

NCYBA may collect and use data for the following purposes:

1. Research on youth issues, governance, public participation, and community development;
2. Public participation activities, including budget advocacy, civic education, and community consultations;
3. Surveys, needs assessments, and baseline studies;
4. Monitoring, evaluation, accountability, and learning (MEAL/MEL);
5. Governance analysis and policy advocacy; and
6. Publication of findings, reports, and advocacy materials.

9.2 Research Ethics and Safeguards

1. All research involving personal data shall be designed and conducted in accordance with ethical research principles, including respect for participants, informed consent, confidentiality, and do no harm;
2. Research participants shall be informed of the purpose of the research, how their data will be used, who will have access, how findings will be published, and their right to withdraw;
3. Research instruments shall be reviewed to ensure data minimization and to avoid collecting unnecessary sensitive information;
4. Where research involves vulnerable populations, including children, persons with disabilities, or marginalized groups, additional safeguards shall apply;
5. Research findings shall be published in a manner that protects participant identity unless explicit consent for attribution has been obtained.

9.3 Anonymisation and Aggregation

- (a) Wherever practicable, research and advocacy data shall be anonymized or aggregated before publication or sharing;



- (b) Individual-level personal data shall not be published in public reports, policy briefs, or media materials without explicit consent;
- (c) Case studies and testimonials used in advocacy shall be reviewed to ensure that identifying details are removed or obscured unless the data subject has expressly authorized identification.

9.4 Responsible Presentation

- (a) Data used in advocacy shall be presented accurately and in context. NCYBA shall not manipulate, misrepresent, or selectively present data to mislead audiences;
- (b) Community-level data shall not be presented in ways that stigmatize, stereotype, or expose specific individuals or groups to harm;
- (c) Advocacy materials shall distinguish between verified data and anecdotal evidence, and shall cite sources appropriately.

10. PHOTOGRAPHS, VIDEOS, AUDIO, AND TESTIMONIALS

10.1 General Principles

NCYBA recognizes that visual and audio materials are powerful tools for documentation, reporting, and advocacy. However, the capture and use of such materials involve significant privacy considerations. NCYBA shall obtain appropriate consent, respect dignity, and prevent contextual misuse.

10.2 Consent Requirements

- (a) Event photography and videography: Where photography or filming is planned at events, participants shall be notified in advance through event notices, signage, or registration materials. Individuals who do not wish to be photographed shall be able to opt out, and NCYBA shall make reasonable efforts to accommodate such requests;
- (b) Promotional and donor materials: Specific consent shall be obtained for the use of images, videos, or audio in promotional materials, donor reports, websites, and social media, using the Multimedia Consent Form;
- (c) Testimonials: Written, audio, or video testimonials require specific consent that clearly states the purpose, intended audience, and duration of use;
- (d) Children: The provisions of Section 10(4) of Data Protection Act, 2019 apply. No photograph, video, or audio of a child shall be used without parental or guardian consent.

10.3 Event Notices

For public events where photography is anticipated, NCYBA shall display clear notices at entrances and registration points informing attendees that photography or filming is taking place, the purpose, and how to opt out.

10.4 Withdrawal and Deletion

11.4.1: Data subjects may withdraw consent for the use of their image, voice, or testimony at any time by contacting the Data Protection Officer;

11.4.2: Upon withdrawal, NCYBA shall cease using the material in future publications and shall make reasonable efforts to remove it from platforms within its control. NCYBA shall inform the data subject that already printed materials or third-party publications may not be retrievable;



11.4.3: Sensitive personal stories or testimonies shall be stored securely and shall not be retained indefinitely if the purpose for which they were collected has ended.

10.5 Contextual Misuse

NCYBA shall not use images, videos, or testimonials in ways that misrepresent the context, exploit the subject, or cause embarrassment or harm. Images shall not be digitally altered to mislead viewers about circumstances or conditions.

11. DATA ACCESS AND ROLE-BASED PERMISSIONS

11.1 Principle of Least Privilege

NCYBA adopts the principle of least privilege: individuals shall have access only to the personal data necessary to perform their specific responsibilities. Access shall not be granted broadly or by default.

11.2 Access Categories

Access to NCYBA data systems shall be categorized as follows:

- (a) Full administrative access: Reserved for designated ICT administrators and senior leadership for system management purposes. Such access shall be logged and reviewed periodically;
- (b) Programme access: Granted to programme and project managers for data related to their specific programmes. Programme staff shall not access data from other programmes without authorization;
- (c) Limited operational access: Granted to field staff, enumerators, and volunteers for data entry, verification, or communication within their assigned scope;
- (d) Read-only access: Granted to personnel who require visibility into data for reporting, monitoring, or oversight but do not need to modify records;
- (e) Temporary access: Granted for specific projects or time-bound activities. Temporary access shall be automatically revoked at the end of the designated period unless renewed.

11.3 User Account Management

- (a) Every individual with access to NCYBA data systems shall have a unique user account. Shared accounts are prohibited;
- (b) Strong passwords shall be required in accordance with applicable information security standards and NCYBA's internal information security policies and procedures. ;
- (c) Multi-factor authentication (MFA) shall be enabled on all systems that support it, particularly email, cloud storage, and database platforms;
- (d) Passwords shall not be shared, written down in accessible locations, or transmitted through unsecured channels;



- (e) Access rights shall be reviewed at least every six months, and immediately upon role changes, exits, or suspected compromise.

11.4 Immediate Revocation

Access to all NCYBA data systems shall be revoked immediately when:

- (a) A staff member, volunteer, or contractor exits the organization or completes their engagement;
- (b) A person's role changes such that they no longer require the access previously granted;
- (c) Unauthorized access or policy violation is suspected; or
- (d) A device or account is lost, stolen, or compromised.



12. DATA SECURITY AND INFORMATION SECURITY

12.1 Digital Security

NCYBA shall implement the following minimum digital security measures:

1. **Strong passwords:** All accounts shall use passwords of at least 12 characters, incorporating uppercase and lowercase letters, numbers, and symbols. Passwords shall be changed at least every 90 days or immediately upon suspected compromise;
2. **Multi-factor authentication (MFA):** MFA shall be enabled on all critical systems including email, cloud storage, financial platforms, and membership databases;
3. **Device protection:** All institutional devices shall have screen locks activated after a maximum of 5 minutes of inactivity. Devices shall not be left unattended in public or unsecured locations;
4. **Encryption:** Sensitive personal data stored on laptops, external drives, or portable devices shall be encrypted where technically feasible. Data transmitted over networks shall be encrypted where possible;
5. **Secure backups:** Institutional data shall be backed up regularly to approved secure locations. Backups shall be tested periodically to ensure recoverability;
6. **Software updates:** All devices and applications shall be kept up to date with security patches. Automatic updates shall be enabled where available;
7. **Antivirus and malware protection:** Approved antivirus and anti-malware software shall be installed and maintained on all devices. Suspicious files or links shall not be opened;
8. **Secure cloud storage:** Only approved cloud storage platforms shall be used for institutional data. Platform configurations shall be reviewed to ensure appropriate sharing permissions and access controls.

12.2 Physical Security

- (a) **Locked storage:** Physical files containing personal data shall be stored in locked cabinets or rooms when not in use. Keys and combinations shall be accessible only to authorized personnel;
- (b) **Restricted access:** Areas where physical records are stored or processed shall be restricted to authorized staff. Visitors shall be supervised;

- (c) **Secure destruction:** Physical documents no longer required shall be shredded, incinerated, or otherwise rendered irretrievable before disposal. Standard waste bins shall not be used for sensitive documents;
- (d) **Clean desk principles:** Staff and volunteers shall not leave documents, devices, or removable media containing personal data visible on desks when unattended or at the end of the workday.

123 Mobile Devices

- (a) All mobile devices (phones, tablets, laptops) used to access or store NCYBA data shall have screen locks (PIN, password, or biometric);
- (b) Where available, device encryption and remote wiping capabilities shall be enabled;
- (c) Lost or stolen devices shall be reported to the Data Protection Officer and ICT administrator immediately to enable remote wiping or account revocation;
- (d) Personal devices used for NCYBA work shall meet the same security standards as institutional devices, and NCYBA data shall be segregated from personal data where practicable.

12.4 Communication Platforms

- (a) **Email:** Sensitive personal data shall not be sent via email unless necessary. Where email is used, recipients shall be verified, and attachments containing sensitive data shall be password-protected or encrypted where feasible;
- (b) **WhatsApp, Telegram, and messaging apps:** These platforms shall not be used to share sensitive personal data, membership lists, or participant information unless no reasonable alternative exists and the data is minimized. Even then, such sharing shall be authorized and documented;
- (c) **Google Workspace or equivalent:** Approved collaborative platforms shall be configured with appropriate access controls. Shared drives shall not be openly accessible to all users unless specifically designated for public materials;
- (d) **Convenience must not override data protection:** Staff and volunteers shall not use personal email accounts, messaging apps, or unapproved platforms to transmit or store institutional data simply because they are convenient.

13. DATA SHARING AND THIRD-PARTY MANAGEMENT

13.1 General Principles

NCYBA shall share personal data with third parties only where:

- (a) There is a lawful basis for sharing;
- (b) The sharing is necessary and proportionate to a defined purpose;
- (c) Appropriate safeguards are in place; and
- (d) The data shared is limited to the minimum necessary.

13.2 Categories of Third Parties

Data sharing may occur with the following categories of third parties, subject to the safeguards in this section:

- (a) Donors and funders: For reporting, verification, and audit purposes. Shared data shall be anonymized or aggregated where possible, and donor data processing agreements shall be in place;
- (b) Government institutions: Where required by law or for legitimate public participation purposes, such as submitting participant lists for official programmes. Sharing shall be documented and limited to legal requirements;
- (c) Research partners: For collaborative research, subject to research ethics approvals, data processing agreements, and confidentiality obligations;
- (d) Consultants and service providers: For specific services such as monitoring and evaluation, ICT support, or financial management. Such providers shall process data only on documented instructions from NCYBA;
- (e) Technology providers: Cloud services, database hosts, and software providers that process data on NCYBA's behalf. These shall be vetted for security and contracted under data processing agreements;
- (f) Implementing partners: Organizations collaborating with NCYBA on joint programmes, subject to written agreements defining data responsibilities.

13.3 Safeguards for Data Sharing

Before sharing personal data with any third party, NCYBA shall ensure:

- (a) A **defined purpose** for sharing is documented;
- (b) Only the **minimum necessary data** is shared;

- (c) The third party is bound by confidentiality obligations, preferably through a written Data Processing Agreement (DPA);
- (d) The third party implements appropriate **technical and organizational security measures**;
- (e) Restrictions on onward sharing are communicated and contractually enforced, prohibiting the third party from sharing NCYBA data with others without written consent;
- (f) **Audit rights** are reserved, allowing NCYBA to verify the third party's compliance; and
- (g) **Return or deletion of data** is required upon termination of the relationship or completion of the purpose.

13.4 Data Processing Agreements

All third parties that process personal data on behalf of NCYBA shall enter into a Data Processing Agreement (DPA) before any data transfer. The DPA shall specify:

- (a) The subject matter, duration, nature, and purpose of processing;
- (b) The categories of data subjects and data involved;
- (c) The processor's obligation to process data only on documented instructions from NCYBA;
- (d) Confidentiality commitments;
- (e) Security measures;
- (f) Sub-processor governance, where applicable;
- (g) Breach notification obligations, remedies and repercussions;
- (h) Assistance with data subject requests;
- (i) Return or deletion of data upon termination; and
- (j) Audit and inspection rights.

14 CROSS-BORDER DATA TRANSFERS

14.1 Applicability

This section applies where NCYBA transfers personal data from Kenya to another country or international organization, including through the use of international cloud service providers, donor platforms, software-as-a-service (SaaS) tools, or research collaborations.

14.2 Legal and Institutional Safeguards

NCYBA data controller or data processor may transfer personal data to another country only where

- (a) the data controller or data processor has given proof to the Data Commissioner on the appropriate safeguards with respect to the security and protection of the personal data;
- (b) the data controller or data processor has given proof to the Data Commissioner of the appropriate safeguards with respect to the security and protection of personal data, and the appropriate safeguards including jurisdictions with commensurate data protection laws;
- (c) the transfer is necessary—
 - (i) for the performance of a contract between the data subject and the data controller or data processor or implementation of pre-contractual measures taken at the data subject's request;
 - (ii) for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person;
 - (iii) for any matter of public interest;
 - (iv) for the establishment, exercise or defence of a legal claim;
 - (v) in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or
 - (vi) for the purpose of 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.

14.3 Cloud and Technology Services

- (a) NCYBA's use of international cloud platforms (such as Google Workspace, Microsoft 365, or similar) for institutional data is permitted provided that the platforms are configured securely and the provider's data processing terms are reviewed;
- (b) Programme staff shall not use personal cloud accounts or unapproved international platforms to store or process NCYBA data;
- (c) The Data Protection Officer shall maintain a register of all international platforms and services used for personal data processing, including the country where data is stored or processed.

15. DATA RETENTION AND DISPOSAL

15.1 Data Lifecycle Approach

NCYBA adopts a formal data lifecycle approach. Personal data shall be retained only for as long as necessary to fulfil the purpose for which it was collected, to comply with legal obligations, to resolve disputes, or to enforce agreements. When data is no longer required, it shall be securely disposed of.

15.2 Retention Schedule

NCYBA shall maintain a Data Retention Schedule as indicated in Annex C in this policy. The schedule shall specify minimum and maximum retention periods for each category of data, taking into account:

- (a) Programme data: Retained for the duration of the programme and a defined period thereafter for evaluation and audit;
- (b) Membership records: Retained for the duration of membership and a defined period thereafter for governance and legal purposes;
- (c) HR and payroll records: Retained in accordance with the Employment Act and tax law requirements;
- (d) Financial and donor records: Retained for the period required by the Kenya Revenue Authority and donor audit requirements;
- (e) Research data: Retained for the period necessary to verify research integrity, publish findings, and comply with ethical obligations;
- (f) Governance records: Retained permanently or for extended periods as required by law and institutional memory;
- (g) Health and incident records: Retained for the period necessary to meet safeguarding, insurance, and legal liability requirements;
- (h) Photographs, videos, and audio: Retained in accordance with the consent obtained and the purpose of collection.

15.3 Periodic Review

The Data Protection Officer shall conduct a periodic review of stored data at least annually to identify data that has exceeded its retention period or is no longer necessary. Programme managers shall be consulted before disposal to confirm operational needs.

15.4 Secure Disposal

When personal data is no longer required, NCYBA shall ensure its secure disposal through:

- (a) **Digital data:** Secure deletion using methods that render data irretrievable, including permanent deletion from systems, secure wiping of storage devices, and, where applicable, destruction of encryption keys;
- (b) **Physical documents:** Shredding, incineration, or pulping to render documents unreadable and irretrievable;
- (c) **Anonymisation:** Where retention of insights or aggregated data is necessary for historical, statistical, or research purposes, individual-level data shall be anonymized before disposal of identifiable records. In accordance with Annex C

15.5 Disposal Log

All disposals of personal data shall be documented in a Disposal Log, recording:

- Date of disposal;
- Category and description of data disposed;
- Volume or quantity;
- Method of disposal;
- Names of witnesses (where required);
- Authorization by the Data Protection Officer or designated officer.

16. DATA SUBJECT RIGHTS

16.1 Rights of Data Subjects

Subject to applicable law, data subjects have the following rights regarding their personal data processed by NCYBA:

- (a) **Right to be informed:** The right to know that their data is being collected, the purposes, the lawful basis, and their rights;
- (b) **Right of access:** The right to obtain confirmation that their data is being processed and to access a copy of their data;
- (c) **Right to rectification:** The right to have inaccurate or incomplete data corrected without undue delay;
- (d) **Right to erasure ('right to be forgotten'):** The right to request deletion of their data where there is no compelling reason for continued processing, subject to legal and operational constraints;
- (e) **Right to restrict processing:** The right to request the limitation of processing in certain circumstances;
- (f) **Right to data portability:** The right to receive their data in a structured, commonly used, and machine-readable format, where technically feasible;
- (g) **Right to object:** The right to object to processing based on legitimate interests or for direct marketing purposes;
- (h) **Right to withdraw consent:** The right to withdraw consent at any time, where consent is the lawful basis; and
- (i) **Right to lodge a complaint:** The right to complain to the NCYBA Data Protection Officer if they believe their rights have been violated.

16.2 Exercising Rights

- (a) Data subjects may exercise their rights by submitting a request to the Data Protection Officer using the Data Subject Request Form or any written communication clearly indicating the nature of the request;
- (b) NCYBA shall verify the identity of the requestor before processing the request to prevent unauthorized disclosure;
- (c) NCYBA shall respond to data subject requests within 30 days of receipt. Where a request is complex or numerous, this period may be extended by two months, with notification to the data subject;

- (d) Where NCYBA cannot comply with a request, it shall inform the data subject of the reasons, their right to appeal internally, and their right to lodge a complaint with the ODPC;
- (e) NCYBA shall not charge a fee for responding to requests unless the request is manifestly unfounded or excessive.

16.3 Requests Relating to Children

Requests relating to children's data may be made by the child (if sufficiently mature), a parent, or a guardian. NCYBA shall verify the relationship and authority of the person making the request.

17. DATA BREACH AND INCIDENT MANAGEMENT

17.1 Definition and Examples

A **data breach** is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data. Examples include:

- (a) Lost or stolen laptops, phones, or storage devices containing personal data;
- (b) Hacked or compromised email, database, or cloud accounts;
- (c) Accidental email disclosure (sending personal data to the wrong recipient);
- (d) Unauthorized database access by internal or external actors;
- (e) Misplaced or stolen physical files;
- (f) Ransomware, malware, or phishing incidents affecting institutional data;
- (g) Unauthorized sharing of participant or membership information through informal channels;
- (h) Improper disposal of physical or digital records leading to exposure.

17.2 Breach Response Process

NCYBA shall respond to data breaches through the following structured process:

Step 1: Detect

- Any personnel who suspects or becomes aware of a data breach shall report it immediately to the Data Protection Officer.
- The Data Protection Officer shall record the incident and activate the breach response protocol.

Step 2: Contain

- Take immediate steps to prevent further loss or exposure, including revoking compromised credentials, isolating affected systems, recovering exposed data where possible, and securing physical areas.
- Preserve evidence for investigation.

Step 3: Assess

- Determine what categories of data were affected, the number of data subjects potentially impacted, the severity of the breach, and the likelihood of resulting harm.
- Classify the breach risk level as Low, Medium, or High.

Step 4: Notify

- If the breach is likely to result in a risk to the rights and freedoms of data subjects, notify the Office of the Data Protection Commissioner (ODPC) within 72 hours of becoming aware of the breach, where required by law.
- If the breach poses a high risk to data subjects, notify affected individuals without undue delay, providing clear information about the breach, the data involved, the likely consequences, and the measures taken.
- The Board shall be informed of all Medium and High risk breaches.

Step 5: Recover

- Restore affected systems from secure backups where necessary.
- Implement additional security measures to prevent recurrence.
- Coordinate with law enforcement where criminal activity is suspected.

Step 6: Learn

- Conduct a post-incident review to identify root causes and lessons learned.
- Update policies, procedures, and training as necessary.
- Document the incident, response actions, and outcomes in the Incident Register.

17.3 Documentation

All data breaches shall be documented, including:

- Date and time of detection;
- Description of the breach;
- Data categories and number of subjects affected;
- Risk assessment;
- Notification actions taken;



- Remedial measures implemented; and
- Review findings.

18. GOVERNANCE STRUCTURE AND RESPONSIBILITIES

18.1 Governing Board

The Governing Board bears ultimate accountability for data protection governance. (A Data Governance Committee Shall be set up).

Its responsibilities include:

- (a) Approving this policy and significant amendments;
- (b) Ensuring that adequate resources are allocated for data protection compliance;
- (c) Receiving reports from the Data Protection Officer on compliance status, incidents, and risks;
- (d) Overseeing the organizational response to serious data breaches;
- (e) Ensuring that data protection is integrated into organizational strategy and risk management; and
- (f) Holding Executive Leadership accountable for implementation.

18.2 Executive Leadership

Executive Leadership (Secretariat, Coordinator, or equivalent) is responsible for:

- (a) Implementing this policy across all programmes and operations;
- (b) Resourcing data protection activities, including training, systems, and personnel;
- (c) Appointing and supporting the Data Protection Officer;
- (d) Ensuring that programme designs incorporate data protection by design;
- (e) Enforcing compliance through management oversight; and
- (f) Reporting to the Board on data protection performance.

18.3 Data Protection Officer or Designated Data Protection Lead

NCYBA shall designate at least one Data Protection Officer (DPO) or Data Protection Lead. The DPO shall:

- (a) Monitor internal compliance with this policy and applicable data protection law;
- (b) Provide advice and guidance to the Board, management, staff, and volunteers on data protection matters;
- (c) Serve as the point of contact for the Office of the Data Protection Commissioner (ODPC);
- (d) Serve as the point of contact for data subjects exercising their rights;
- (e) Conduct and coordinate Data Protection Impact Assessments;

- (f) Manage data breach response and incident documentation;
- (g) Develop and deliver training and awareness programmes;
- (h) Maintain the Data Processing Register and related documentation;
- (i) Conduct periodic compliance audits and reviews; and
- (j) Report directly to the Board or Executive Leadership with independence from operational pressures.

The DPO shall have adequate time, authority, and resources to fulfil these responsibilities and shall not be penalized for performing their duties.

18.4 Programme and Project Managers

Programme and Project Managers are responsible for:

- (a) Ensuring that data collection, use, and storage within their programmes comply with this policy;
- (b) Reviewing and approving research instruments, consent forms, and data collection tools;
- (c) Supervising staff, volunteers, and enumerators to ensure proper data handling;
- (d) Reporting data breaches or suspected violations within their programmes;
- (e) Ensuring programme data is retained and disposed of in accordance with the Data Retention Schedule.

18.5 ICT or Systems Administrators

ICT or Systems Administrators are responsible for:

- (a) Implementing and maintaining technical security measures;
- (b) Managing user accounts, access controls, and authentication systems;
- (c) Ensuring secure configuration of databases, cloud services, and networks;
- (d) Managing backups, encryption, and software updates;
- (e) Supporting breach containment and recovery; and
- (f) Advising on secure technology choices.

18.6 Staff and Volunteers

All staff and volunteers shall:

- (a) Complete mandatory data protection training before handling personal data;
- (b) Process personal data only for authorized NCYBA purposes;



- (c) Follow all security procedures, including password policies, device protection, and communication rules;
- (d) Report actual or suspected data breaches immediately;
- (e) Maintain confidentiality of all personal data they access; and
- (f) Return or delete all NCYBA data upon exit.

18.7 Third Parties

Third parties processing data on behalf of NCYBA shall:

- (a) Comply with the terms of their Data Processing Agreement;
- (b) Implement appropriate technical and organizational security measures;
- (c) Notify NCYBA of any data breach without undue delay;
- (d) Assist NCYBA in responding to data subject requests; and
- (e) Return or delete all NCYBA data upon termination of the agreement.

19. DATA PROTECTION IMPACT AND RISK ASSESSMENTS

19.1 When to Conduct an Internal and External Assessment

NCYBA shall conduct an internal External Data Protection Impact Assessment (DPIA) before undertaking processing activities that are likely to result in a high risk to the rights and freedoms of data subjects. Such activities include:

- (a) Large-scale surveys or data collection involving significant numbers of individuals;
- (b) The introduction of new digital platforms, databases, or mobile applications;
- (c) The collection of sensitive personal data, including health data or biometric data;
- (d) The implementation of biometric identification or authentication systems;
- (e) High-risk research involving vulnerable populations;
- (f) The creation or significant expansion of membership databases;
- (g) New data-sharing partnerships or third-party processing arrangements;
- (h) Systematic monitoring, tracking, or profiling of individuals; and
- (i) Any other processing that the Data Protection Officer determines requires assessment.

19.2 Assessment Content

A DPIA shall include:

- (a) A systematic description of the processing activity, its purposes, and the data involved;
- (b) An assessment of the necessity and proportionality of the processing;
- (c) An evaluation of the risks to the rights and freedoms of data subjects;
- (d) The measures envisaged to address the risks, including safeguards, security measures, and mechanisms to ensure protection of personal data;
- (e) Consultation with relevant stakeholders where appropriate; and
- (f) A conclusion on whether the processing should proceed, proceed with conditions, or not proceed.

19.3 Review

DPIAs shall be reviewed periodically and whenever there is a significant change to the processing activity.

20. DATA ETHICS AND RESPONSIBLE USE

20.1 Ethical Framework

NCYBA commits to an ethical framework that goes beyond legal compliance. This framework is based on the following principles:

- (a) Do no harm: Data shall not be collected, used, or shared in ways that could cause physical, psychological, social, or economic harm to individuals or communities;
- (b) Respect for dignity: Data subjects shall be treated with respect. Their stories, images, and information shall not be exploited or used in ways that demean or dehumanize;
- (c) Avoidance of discrimination: Data shall not be used to discriminate against, stereotype, or marginalize individuals or groups based on ethnicity, religion, gender, disability, economic status, or other protected characteristics;
- (d) Prevention of manipulation: NCYBA data shall not be used to manipulate, coerce, or unduly influence young people or community members for unethical reasons such as political purposes, performance pressure, personal gain or advocacy misrepresentation.
- (e) Avoidance of exploitative data extraction: NCYBA shall not extract data from communities purely for institutional benefit without ensuring that the community also benefits and that their trust is respected;
- (f) Responsible use of data in advocacy: Advocacy based on data shall be honest, contextual, and shall not misrepresent individual experiences or community realities;
- (g) Transparency: NCYBA shall be open about what data it collects, why, and how it is used; and
- (h) Community trust: All data practices shall be evaluated against their impact on community trust. Loss of trust undermines NCYBA's mission and shall be avoided.

20.2 Ethical Decision-Making

When considering whether to collect or use data, NCYBA personnel shall ask:

- (a) Is this collection necessary and justified?
- (b) Could this data, if misused, harm the individual or community?
- (c) Are we being transparent about our intentions?
- (d) Are we respecting the dignity and autonomy of data subjects?

(e) Would this practice withstand public scrutiny?

Just because data can legally or technically be collected does not automatically mean that NCYBA should collect it.

21.3 Prohibited Data Practices

The following practices are strictly prohibited:

- (a) Selling personal data to any third party for financial gain or otherwise;
- (b) Sharing personal data for personal benefit, commercial advantage, or political advancement;
- (c) Using membership databases for unauthorized political campaigns, candidate promotion, or party mobilization;
- (d) Sharing personal information through informal communication channels (such as personal WhatsApp, email, or social media) without justification and authorization;
- (e) Collecting unnecessary sensitive personal data without compelling justification and appropriate safeguards;
- (f) Using another person's account credentials to access NCYBA systems;
- (g) Sharing passwords, PINs, or authentication codes with colleagues, friends, or family;
- (h) Downloading institutional databases or bulk personal data onto personal devices, cloud accounts, or storage media without authorization;
- (i) Publishing personal information in public reports, social media, or promotional materials without an appropriate lawful basis and, where required, consent;
- (j) Retaining personal data indefinitely without justification or beyond the periods specified in the Data Retention Schedule;
- (k) Accessing personal data out of curiosity or for reasons unrelated to official duties;
- (l) Altering, deleting, or falsifying personal data without authorization;
- (m) Failing to report a known or suspected data breach;
- (n) Removing physical documents or digital files containing personal data from NCYBA premises without authorization; and
- (o) Using NCYBA data to harass, intimidate, or discriminate against any individual.

21. TRAINING AND ORGANISATIONAL CAPACITY

21.1 Training Requirements

NCYBA shall ensure that all personnel receive appropriate data protection training:

- (a) Staff induction: All new staff shall complete data protection training as part of their orientation before accessing personal data;
- (b) Volunteer orientation: All volunteers shall receive data protection orientation before commencing activities involving personal data;
- (c) Periodic training: All personnel shall receive refresher training at least annually, or more frequently if significant policy changes or incidents occur;
- (d) Researcher and enumerator training: Individuals conducting research or field data collection shall receive specialized training on research ethics, consent procedures, data minimization, and secure handling of field data;
- (e) Cybersecurity awareness: All personnel shall receive training on recognizing phishing, malware, and social engineering threats, and on secure password practices;
- (f) Incident reporting awareness: All personnel shall be trained on how to recognize and report data breaches and suspected violations.

21.2 Training Records

NCYBA shall maintain records of training completion, including dates, participants, and topics covered.

21.3 Capacity Building

The Data Protection Officer shall identify capacity gaps and recommend resources, tools, or external support to strengthen NCYBA's data protection capabilities.

22. COMPLIANCE, MONITORING, AND AUDIT

22.1 Periodic Compliance Reviews

The Data Protection Officer shall conduct periodic compliance reviews to assess adherence to this policy. Reviews shall include:

- (a) Examination of the Data Processing Register for completeness and accuracy;
- (b) Review of consent forms and data collection notices;
- (c) Assessment of access controls and user account management;
- (d) Verification of data retention and disposal practices;
- (e) Review of third-party data processing agreements;
- (f) Inspection of physical and digital security measures; and
- (g) Interviews or surveys with staff and volunteers.

22.2 Access Audits

User access rights shall be audited at least every six months to ensure that permissions remain appropriate and that former personnel no longer have access.

22.3 Database Reviews

Membership and programme databases shall be reviewed annually to identify obsolete data, unauthorized access, or configuration weaknesses.

22.4 Security Assessments

Technical security assessments shall be conducted periodically, including review of cloud configurations, backup integrity, and vulnerability to common threats.

22.5 Partner Compliance Reviews

Third parties processing NCYBA data shall be reviewed periodically to verify compliance with their contractual obligations. This may include requests for self-assessments, document review, or, where warranted, on-site verification.

22.6 Internal Reporting

The Data Protection Officer shall report findings from compliance reviews to Executive Leadership and the Board at least annually, or more frequently if serious issues are identified.



22.7 Corrective Action

Where violations or weaknesses are identified, NCYBA shall implement corrective action, which may include:

- Additional training;
- System reconfiguration;
- Policy clarification;
- Disciplinary measures (see Section 23); and
- Reporting to relevant authorities where required.

23. POLICY VIOLATIONS AND DISCIPLINARY ACTION

23.1 Proportionality

Violations of this policy shall be addressed proportionally, taking into account the severity of the violation, whether it was intentional or negligent, the harm caused or risked, and any mitigating factors.

23.2 Range of Responses

Responses to policy violations may include:

- (a) Training or corrective action: For minor or first-time violations arising from lack of awareness, additional training or a written warning may be appropriate;
- (b) Suspension of access: For violations involving unauthorized access, sharing, or security failures, the individual's access to data systems may be suspended pending investigation;
- (c) Internal disciplinary procedures: For serious or repeated violations, NCYBA shall initiate formal disciplinary procedures in accordance with staff or volunteer policies;
- (d) Termination of contractual relationships: For severe violations, particularly those involving intentional misuse, unauthorized sharing, or theft of data, NCYBA may terminate employment, volunteer engagement, or contractual relationships;
- (e) Reporting to relevant authorities: Where a violation constitutes a criminal offense or serious breach of data protection law, NCYBA may report the matter to the Office of the Data Protection Commissioner, law enforcement, or other relevant authorities; and
- (f) Civil liability: NCYBA reserves the right to pursue civil remedies for damages resulting from policy violations.

23.3 Whistleblower Protection

Personnel who report suspected violations in good faith shall be protected from retaliation. Reports may be made through the channels identified in Section 24.

24. COMPLAINTS AND REPORTING CHANNELS

24.1 Privacy Concerns and Complaints

Individuals who wish to raise privacy concerns, report suspected misuse of data, or submit complaints may do so through the following channels:

Data Protection Officer: Paul Olunga Agutu

Email: [Nandibunge2017@gmail.com]

Phone: [0719577214]

Postal Address: [P.O Box 600-30300 Kapsabet NCYBA Office Address]

(b) Executive Leadership: Nicholas Kibet 0710679877]

(c) Board Chairperson: [Nicholas Kibet 0710679877]

24.2 Reporting Data Security Incidents

Suspected data breaches or security incidents shall be reported immediately to the Data Protection Officer through any of the above channels. Reports may also be made in person or through any available communication method if urgent.

24.3 Anonymous Reporting

Where individuals are uncomfortable identifying themselves, anonymous reports may be submitted through suggestion address/email. Anonymous reports will be investigated to the extent possible, though follow-up may be limited.

24.4 Response to Complaints

NCYBA shall acknowledge receipt of complaints within 3 working days and shall provide a substantive response within 21 working days, or within a reasonable timeframe for complex matters. Complainants shall be informed of their right to escalate to the Office of the Data Protection Commissioner if dissatisfied.

25. REVIEW AND AMENDMENT OF THE POLICY

25.1 Regular Review

This policy shall be reviewed at least annually to ensure that it remains accurate, effective, and aligned with applicable law and organizational practice.

25.2 Triggered Review

A review shall also be conducted:

- (a) When there are significant changes in Kenyan data protection law or regulatory guidance;
- (b) When NCYBA introduces major new technologies, databases, or data systems;
- (c) Following a significant data breach or security incident;
- (d) When organizational activities materially change, such as expansion into new programme areas or geographic locations;
- (e) When donor requirements or partnership obligations necessitate policy updates; and
- (f) When weaknesses are identified through compliance monitoring or audit.
- (g) After a DPIA has been conducted

25.3 Amendment Process

Amendments to this policy shall be proposed by the Data Protection Officer, reviewed by Executive Leadership, and approved by the Governing Board. All amendments shall be documented in the version history, communicated to all personnel, and incorporated into training materials.

26. RELATED DOCUMENTS

This Policy is supported by the following operational documents and templates, which shall be developed, maintained, and used in conjunction with this Policy:

- (a) **Data Retention Schedule (Annex C)** — sets out retention periods and disposal methods for each category of data;
- (b) **Data Breach Response Procedure (Annex F)** — provides detailed step-by-step guidance for responding to data breaches;
- (c) **Data Subject Request Procedure** — operational guidance for receiving, assessing, and responding to data subject rights requests;
- (d) **Consent Management Guidelines** — guidance on obtaining, documenting, and managing consent;
- (e) **Research and Data Collection Guidelines** — ethical and operational guidance for research activities;
- (f) **Information Security Procedure** — detailed technical and operational security requirements; g) **ICT Acceptable Use Policy** — rules for the use of NCYBA's ICT systems and devices;
- (g) **Third-Party Data Processing Agreement Template (Annex G)** — standard contract for third-party data processors;
- (h) **Data Protection Impact Assessment Template** — template for conducting DPIAs;
- (i) **Data Incident Reporting Form** — standard form for reporting breaches and incidents;
- (j) **Staff and Volunteer Exit Checklist** — ensures that access is revoked and data returned when individuals leave NCYBA;
- (k) **Event Photography Notice Template** — standard notice for display at events; and
- (l) Any other documents that Executive Leadership determines are necessary to support compliance with this Policy.

ANNEX TEMPLATES FOR NCYBA DATA PROTECTION POLICY

ANNEX A: DATA INVENTORY & PROCESSING REGISTER TEMPLATE

NCYBA DATA PROCESSING REGISTER

Processing Activity	Data Categories	Purpose	Lawful Basis	Data Subjects	Retention Period	Storage Location	Security Measures	Third-Party Sharing (Y/N)	DPA in Place
Youth Program Registration	Name, Age, ID No., Phone, Email, Location	Participant enrollment, communication	Consent (B1)	Youth (13-35)	3 years post-program	Google Drive (encrypted), Physical files (locked)	Password protection, access controls	No	N/A
Donor Management	Name, Contact, Payment Details	Fundraising, receipts, updates	Legitimate Interests (D)	Donors	7 years for audit	QuickBooks, encrypted spreadsheet	Encryption, 2FA	Yes (bank)	Yes (G)
Event Photography	Images, Video	Marketing, reporting, social media	Consent (B3)	Participants	Indefinite (with consent)	External hard drive, cloud	Password protection	No	N/A
Employee Records	Name, ID, KRA PIN, Bank Details, Contracts	HR management, payroll, compliance	Legal obligation	Staff	7 years post-employment	Locked cabinet, password-protected PC	Physical locks, encryption	Yes (KRA, NSSF)	Required by law
Health Data (Special)	Medical conditions, allergies	Emergency care during programs	Explicit consent (B2)	Youth participants	1 year post-program	Separate encrypted file	Encryption, restricted access	No	N/A

ANNEX B1: STANDARD CONSENT FORM TEMPLATE

NCYBA DATA PROCESSING CONSENT FORM: For Participants Aged 18+

Project/Program: _____

Date: _____

I, _____ [Full Name], provide my informed consent to Nandi County Youth Bunge Association (NCYBA) to collect and process my personal data for the following purposes:

1. DATA COLLECTED:

- **Full Name** _____
- **Age/Date of Birth** _____
- **Phone Number** _____
- **Email Address** _____
- **Location/Address** _____
- **Education Level** _____
- **Employment Status** _____
- **Other:** _____

2. PURPOSE OF PROCESSING:

- Program enrollment and management
- Communication about program activities
- Monitoring and evaluation
- Reporting to funders (anonymized where possible)

3. DATA STORAGE & SECURITY:

My data will be stored securely for 3 years after program completion, then securely deleted. NCYBA implements password protection, encryption, and access controls.

4. MY RIGHTS:

I understand I have the right to:

- Access my data
- Correct inaccurate data
- Withdraw this consent anytime
- Request deletion of my data
- Lodge a complaint with the Data Commissioner

5. WITHDRAWAL:

I may withdraw consent by emailing [Nandibunge2017@gmail.com] or calling [0723981919]. Withdrawal does not affect processing that occurred before withdrawal.

CONSENT STATEMENT:

- I AGREE - I have read and understood this form. I consent to NCYBA processing my personal data as described above.
- I DO NOT AGREE

Signature: _____

Date: _____

Witness (NCYBA Staff): _____

Staff ID: _____

ANNEX B2: PARENTAL/GUARDIAN CONSENT FORM TEMPLATE

NCYBA MINOR DATA PROCESSING CONSENT FORM: For Participants Under 18 Years

Child's Name: _____

Age: _____

Date of Birth: _____

Program: _____

I, _____ [Parent/Guardian Name],

Relationship to Child: _____

My ID Number: _____

Contact: _____

Hereby grant permission for NCYBA to collect and process my child's personal data:

DATA COLLECTED:

- Child's name, age, school, health information relevant to participation (e.g., allergies)
- Contact information for emergency purposes
- I consent to general data collection for program participation
- I consent to collection of health data for safety purposes (specify):

PURPOSES:

- Safe participation in youth programs
- Emergency contact if needed
- Program evaluation and reporting

I ACKNOWLEDGE MY CHILD'S RIGHTS:

NCYBA will protect my child's data with enhanced security. I retain the right to access, correct, or request deletion of this data.

CONSENT:

- I AGREE to NCYBA processing my child's data as described.
- I DO NOT AGREE



Signature of Parent/Guardian: _____

Date: _____ **NCYBA Official (Print & Sign):** _____

Date: _____

ANNEX B3: MULTIMEDIA CONSENT & RELEASE FORM

NCYBA PHOTO/VIDEO/AUDIO CONSENT FORM

I, _____ [Full Name],

ID No.: _____

Program/Event: _____

Date: _____

Grant NCYBA permission to capture and use my image, voice, or likeness in photographs, videos, or audio recordings for:

PURPOSES (check all that apply):

- NCYBA website and social media
- Program reports and presentations
- Fundraising and promotional materials
- Training and educational materials
- Media publications (newspapers, TV)

TERMS:

1. I understand I will not be paid for this use.
2. NCYBA may edit, copy, or distribute these materials.
3. Materials may be stored indefinitely unless I request deletion.
4. I may withdraw consent by written notice, but this does not affect already published materials.

SPECIFIC RESTRICTIONS (if any):

- I consent only if my image is not the primary focus
- I consent only for use in [specify, e.g., internal reports only]
- Other: _____

CONSENT:

- I AGREE to the terms above.
- I DO NOT AGREE to my image/voice being recorded or used.

Signature: _____

Date: _____



NCYBA Photographer/Staff: _____

Staff ID: _____

ANNEX C: DATA RETENTION SCHEDULE TEMPLATE

NCYBA DATA RETENTION AND DISPOSAL SCHEDULE

Data Category	Minimum Retention Period	Legal/Operational Basis	Disposal Method	Responsible Officer
Participant Registration Forms	3 years after program ends	Program evaluation, audit trail	Secure shredding	Program Manager
Donor Records & Financial Data	7 years	Tax Law (Kenya Revenue Authority)	Secure shredding, digital wiping	Treasurer
Employee Contracts & Payroll	7 years post-employment	Employment Act, tax requirements	Secure shredding	Chairperson
Health & Incident Records	3 years after participation	Child protection, liability	Incineration or shredding	DPO
Meeting Minutes & Governance	Permanently	Historical record, legal compliance	Digital archive	Secretary
Grant Proposals & Reports	7 years after grant closure	Donor requirements, audit	Secure shredding	Program Manager
CCTV Footage	30 days	Security purposes	Overwrite/delete	Security Officer
Volunteer Applications	1 year after application	Reference for future openings	Shredding	Volunteer Coordinator
Email Correspondence	3 years	Operational reference	Digital deletion	All staff
Photographs/Videos	Indefinite (with consent)	Historical archive	Secure digital storage	Communications Officer

Review annually. Document all disposals in Disposal Log.

DISPOSAL LOG ENTRY:

Date: _____

Data Type: _____

Volume: _____

Disposal Method: _____



Witness 1: _____

Witness 2: _____

Approved by DPO: _____

ANNEX D: LEGITIMATE INTERESTS ASSESSMENT (LIA) TEMPLATE

LIA REFERENCE: LIA-[Number]-[Year]

Processing Activity: _____

Date of Assessment: _____

1. PURPOSE OF PROCESSING

Describe the activity and why it's necessary:

2. NECESSITY TEST

Is this processing necessary for NCYBA's legitimate interests?

- Yes – Explain: _____
- No – Consider alternative basis

3. LEGITIMATE INTERESTS IDENTIFIED

- Program effectiveness and improvement
- Fundraising for youth empowerment
- Fraud prevention and security
- Network and communications administration
- Other: _____

4. IMPACT ASSESSMENT

Potential impact on Data Subjects:

(a) Privacy intrusion level:

- Low
- Medium
- High

(b) Data sensitivity:

- Normal
- Special Category

(c) Reasonable expectations of Data Subjects: _____

Mitigation measures to reduce impact:

- Transparency (privacy notice provided)
- Opt-out mechanism available

- Data minimization applied
- Security safeguards in place
- Regular review scheduled

5. BALANCING TEST

Do NCYBA's interests override individual rights?

- Yes – Justification: _____
- No – Do not proceed on this basis

6. CONCLUSION & ACTION

- Processing is justified under Legitimate Interests
- Processing requires additional safeguards: _____
- Processing is NOT justified – seek alternative basis

Assessed by: _____ (DPO)

Approved by: _____ (Chairperson)

Date: _____

Review Date: _____ (12 months from assessment)

ANNEX E: DATA SUBJECT REQUEST FORM

For individuals to access, correct, or delete their personal data

SECTION 1: DATA SUBJECT DETAILS

Full Name: _____

ID/Passport Number: _____

Contact Phone: _____

Email: _____

Relationship to NCYBA: ☐ Participant ☐ Donor ☐ Staff ☐ Volunteer ☐ Other: _____

SECTION 2: REQUEST TYPE

Select one:

- Access Request – I want to know what data you hold about me
- Correction Request – My data is inaccurate; here are the corrections: _____
- Deletion Request – I want my data deleted (please specify reason): _____
- Withdraw Consent – I withdraw my consent for processing
- Objection to Processing – I object to processing based on legitimate interests
- Portability Request – I want my data in a machine-readable format

SECTION 3: IDENTITY VERIFICATION

To prevent unauthorized access, please provide:

- Copy of ID attached:
 - Yes
 - No
- Recent NCYBA communication referenced: _____

SECTION 4: DECLARATION

I confirm that the information provided is accurate and I am the Data Subject or their authorized representative.

Signature: _____

Date: _____

FOR OFFICIAL USE ONLY

Request Received: _____

Request ID: DS-[Year]-[Number]

Assigned to DPO: _____

Due Date: _____ (30 days from receipt)

Status:

- Pending
- Processing
- Completed
- Denied (Give Reason _____)

Completion Date: _____

Method of Response: _____

ANNEX F: DATA BREACH RESPONSE PLAN & FORM

NCYBA DATA BREACH RESPONSE CHECKLIST

STEP 1: CONTAINMENT (IMMEDIATE ACTION)

- Isolate affected systems
- Revoke compromised access credentials
- Recover any exposed data if possible
- Preserve evidence for investigation

STEP 2: ASSESSMENT (WITHIN 24 HOURS)

Complete Breach Assessment Form:

Date/Time Detected: _____

Detected By: _____

Breach Type: ☐ Unauthorized access ☐ Theft ☐ Loss ☐ Accidental disclosure ☐ Other:

Data Categories Affected: _____

Number of Data Subjects Affected: _____

Risk Level: ☐ Low ☐ Medium ☐ High

Potential Harm: _____

STEP 3: NOTIFICATION DECISION

Report to ODPC within 72 hours if breach poses risk to rights/freedoms:

☐ Report required – DPO to complete ODPC form

☐ Report not required – justification: _____

Notify Data Subjects if high risk:

☐ Notification required – prepare communication

☐ Notification not required – justification: _____

STEP 4: REMEDIATION

Corrective Actions: _____

Preventive Measures: _____

Person Responsible: _____

Due Date: _____



STEP 5: DOCUMENTATION & REVIEW

Breach recorded in Incident Register: [] Yes

Lessons learned session conducted: [] Yes

Policy/procedure updates required: _____

BREACH REPORT FORM

Incident Reference: BR-[Year]-[Number]

Report Prepared by: _____

Date: _____

Approved by DPO: _____

ANNEX G: DATA PROCESSING AGREEMENT TEMPLATE

This Agreement is made between:

Data Controller: Nandi County Youth Bunge Association (NCYBA)

Data Processor: _____ [Company Name]

1. SUBJECT MATTER

The Processor provides [services] and processes personal data on behalf of NCYBA.

2. DATA PROCESSING DETAILS

As described in Appendix 1 – Processing Specifications.

3. PROCESSOR OBLIGATIONS

- (a) Process data only on documented instructions from NCYBA
- (b) Ensure confidentiality
- (c) Implement appropriate technical and organizational security measures
- (d) Notify NCYBA of any data breach within 24 hours
- (e) Assist NCYBA in responding to Data Subject requests
- (f) Delete or return all data after service completion
- (g) Submit to audits by NCYBA or its appointee

4. SUB-PROCESSING

Processors may not engage sub-processors without NCYBA's prior written consent.

5. TERM AND TERMINATION

This Agreement remains in effect for the service duration. Upon termination, the Processor shall return or delete all NCYBA data.

SIGNATURES:

For NCYBA:

Name: _____

Title: Chairperson

Signature: _____

Date: _____

For Processor:

Name: _____

Title: _____



Signature: _____

Date: _____

PROCESSING SPECIFICATIONS

Data Categories: _____

Data Subjects: _____

Purpose: _____

Duration: _____

Security Measures: _____

ANNEX H: STAFF/VOLUNTEER CONFIDENTIALITY UNDERTAKING

NCYBA CONFIDENTIALITY & DATA PROTECTION UNDERTAKING

I, _____, employed/volunteering as _____ at NCYBA, hereby agree to:

1. Complete data protection training before handling any personal data.
2. Process personal data only for authorized NCYBA purposes.
3. Maintain confidentiality of all personal data I access.
4. Use only approved, secure systems and follow password policies.
5. Report data breaches or suspected breaches immediately to a DPO.
6. Return all NCYBA materials (digital and physical) upon termination.
7. Not disclose confidential information during or after my engagement.

I understand that violation may result in disciplinary action, termination, and/or legal proceedings.

Acknowledgment:

- I have received and read the NCYBA Data Protection Policy (Version 1)
- I understand my responsibilities under the Data Protection Act, 2019
- I commit to following NCYBA's data protection procedures

Signature: _____

ID Number: _____

Date: _____

Witness (DPO/Manager): _____

Date: _____

ANNEX I: NCYBA PRIVACY NOTICE TEMPLATE

Who We Are: Nandi County Youth Bunge Association empowers youth through programs and advocacy.

How We Collect Your Data: Through registration forms, events, donations, and website interactions.

Data We Collect: Name, contact details, ID (for programs), payment details (donors), images (with consent).

How We Use Your Data:

- To deliver youth programs
- To communicate about activities
- To process donations and issue receipts
- To improve our services
- To comply with legal obligations

Legal Basis: We process your data based on your consent, legitimate interests, or legal requirements.

Data Sharing: We only share data with trusted partners under strict agreements or when required by law.

Data Security: We implement appropriate technical and organizational security measures.

Your Rights: You have the right to access, correct, delete, or restrict your data. Contact our DPOs to exercise these rights.

Retention: We keep data only as long as necessary for its purpose, as per our retention schedule Annex C

Contact Our DPO: [\[Nandibunge2017@gmail.com\]](mailto:Nandibunge2017@gmail.com) | [\[0723981919\]](tel:0723981919)

Complaints: You may lodge a complaint with the Office of the Data Protection Commissioner, Kenya.

This notice is supplemental to specific consent forms used for different activities.



NANDI COUNTY YOUTH BUNGE ASSOCIATION

Data Protection and Privacy Policy 2026

EMAIL

Nandibunge2017@gmail.com

PHONE

0723981919

POSTAL ADDRESS

P.O. Box 600-30300 Kapsabet

In collaboration with



October 2026