



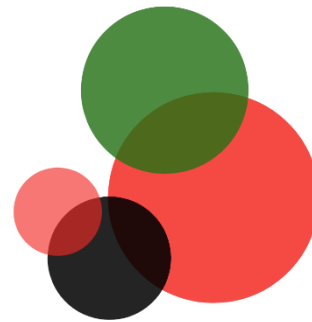
**Youth Projects
Development Platform**

PRIVACY AND DATA PROTECTION POLICY

*A Community of Visionary Youths,
A Platform for Change*

© 2026 Edition

The Youth Projects Development Platform



Youth Projects Development Platform

A Community of Visionary Youths, A Platform for Change

THE PRIVACY AND DATA PROTECTION POLICY

© 2026 Edition

APPROVAL AND SIGNATORIES

This Privacy and Data Protection Policy has been reviewed and approved by the Board of Youth Projects Development Platform (YPDP) and is effective from the date specified in the Document Control section. By approving this Policy, the Board affirms YPDP's commitment to protecting the privacy, confidentiality, security, and rights of individuals whose personal data is processed by or on behalf of the organisation.

Name	Position	Signature	Date
Patience Mumbi	Board Chair	_____	01/09/2026

DOCUMENT CONTROL

Item	Details
Document Title	Privacy and Data Protection Policy
Version	1.0
Effective Date	25 August 2026
Review Cycle	Every 2 Years
Next Review Date	August 2028
Custodian	Data Protection Officer / Designated Data Protection Responsible Person, Youth Projects Development Platform
Approving Authority	YPDP Board

TABLE OF CONTENTS

APPROVAL AND SIGNATORIES.....	iii
DOCUMENT CONTROL	iv
1. INTRODUCTION	1
2.PURPOSE OF THE POLICY	1
3. RESPONSIBILITY.....	2
4. DEFINITIONS AND TERMINOLOGY	2
5. LEGAL AND REGULATORY FRAMEWORK.....	4
6. DATA PROTECTION PRINCIPLES	4
7. PERSONAL DATA COLLECTED AND PROCESSED	5
8. COLLECTION AND PROCESSING OF PERSONAL DATA	8
9. LAWFUL BASIS FOR PROCESSING	10
10. CONSENT AND WITHDRAWAL OF CONSENT	11
11. USE AND DISCLOSURE OF PERSONAL DATA.....	13
12. DATA SUBJECT RIGHTS	16
13. DATA SHARING AND THIRD PARTIES	18
14. CROSS-BORDER/INTERNATIONAL DATA TRANSFERS.....	20
15. DATA SECURITY AND CONFIDENTIALITY	23
16. DATA RETENTION, ARCHIVING AND DISPOSAL.....	26
17. DATA BREACH MANAGEMENT	29
18. ROLES AND RESPONSIBILITIES	34
19. REPORTING, COMPLAINTS AND ENQUIRIES.....	38
20. NON-COMPLIANCE AND CONSEQUENCES	41
21. MONITORING, COMPLIANCE AND POLICY REVIEW	44

1. INTRODUCTION

Youth Projects Development Platform (YPDP) is committed to protecting the privacy, confidentiality, and security of personal data entrusted to it by its staff, volunteers, beneficiaries, members, donors, partners, service providers, and other stakeholders. As a civil society organisation, YPDP recognises that responsible collection, use, storage, sharing, and disposal of personal data is essential to maintaining trust and protecting individual rights.

This Privacy and Data Protection Policy establishes the framework for the lawful, fair, transparent, and secure handling of personal data across YPDP's operations. It sets out the principles, standards, responsibilities, and measures for protecting personal data against unauthorised access, loss, misuse, alteration, disclosure, or destruction. The Policy reflects YPDP's commitment to applicable Zambian data protection requirements and recognised good practices, and promotes a culture of privacy, accountability, confidentiality, and responsible information management.

2. PURPOSE OF THE POLICY

The purpose of this Privacy and Data Protection Policy is to establish a clear framework for the responsible, lawful, and secure handling of personal data by Youth Projects Development Platform (YPDP). The Policy aims to protect the privacy and rights of individuals whose personal data is collected or processed by the organisation and to ensure that such data is handled with appropriate care, confidentiality, and accountability.

Specifically, the Policy seeks to:

- Establish principles and standards for the collection, processing, use, storage, sharing, retention, and disposal of personal data;
- Ensure compliance with applicable data protection and privacy requirements in zambia;
- Safeguard personal data against unauthorised access, loss, misuse, disclosure, alteration, or destruction;
- Clarify the responsibilities of persons who handle personal data on behalf of ydpd; and
- Promote awareness, accountability, and a consistent culture of privacy and data protection across the organisation..

3. RESPONSIBILITY

This Privacy and Data Protection Policy applies to all operations, programmes, projects, and activities of YPDP that involve the collection, processing, use, storage, sharing, retention, or disposal of personal data.

The Policy applies to all individuals acting on behalf of or associated with YPDP, including members of the Board, management, employees, volunteers, interns, consultants, contractors, partners, and other persons who have access to or process personal data on behalf of the organisation.

The Policy covers personal data relating to staff, volunteers, beneficiaries, programme participants, members, donors, partners, service providers, and other stakeholders. It applies to personal data held in both physical and electronic formats, regardless of how or where the data is collected, processed, or stored. All persons and third parties to whom this Policy applies are required to comply with its provisions and to take reasonable measures to protect personal data entrusted to them.

4. DEFINITIONS AND TERMINOLOGY

For the purposes of this Privacy and Data Protection Policy, the following terms shall have the meanings set out below:

Personal Data

Any information relating to an identified or identifiable individual, whether recorded electronically, in writing, or in any other form.

Data Subject

An identified or identifiable individual whose personal data is collected, held, or processed by YPDP.

Data Controller

A person or organisation that determines the purposes for which, and the manner in which, personal data is processed.

Data Processor

A person or organisation that processes personal data on behalf of and under the instructions of a data controller.

Processing

Any operation or set of operations performed on personal data, including collection, recording, organisation, storage, retrieval, use, disclosure, sharing, alteration, restriction, deletion, or destruction.

Consent

A freely given, specific, informed, and unambiguous indication of an individual's wishes by which the individual agrees to the processing of their personal data.

Sensitive or Special Category Personal Data

Personal data that requires enhanced protection because of its nature or the potential harm that may result from its misuse or unauthorised disclosure. This may include information relating to health, biometric data, identity documents, children's data, or other categories recognised as sensitive under applicable law.

Personal Data Breach

A breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to personal data.

Data Protection Officer/Responsible Person

The person designated by YPDP to oversee and coordinate the organisation's compliance with this Policy and applicable data protection requirements.

Data Protection Impact Assessment (DPIA)

A systematic assessment undertaken to identify, evaluate, and manage potential privacy and data protection risks arising from a proposed activity or processing of personal data.

Anonymisation

The process of removing or altering information so that personal data can no longer be used to identify an individual, taking into account the means reasonably likely to be used for identification.

Pseudonymisation

The processing of personal data in such a way that it can no longer be attributed to a specific individual without the use of additional information, which is kept separately and protected by appropriate safeguards.

5. LEGAL AND REGULATORY FRAMEWORK

Youth Projects Development Platform shall implement this Policy in accordance with the applicable laws, regulations, standards, and regulatory guidance governing privacy and the protection of personal data in Zambia. The principal legal framework for this Policy is the Data Protection Act No. 3 of 2021, which provides for the protection and regulation of personal data, including its collection, use, transmission, storage, and processing. The Act also establishes the Data Protection Commissioner and provides for the registration and regulation of data controllers and data processors, their duties, and the rights of data subjects.

YPDP shall also have regard to applicable regulations and guidance issued under the Data Protection Act, including the Data Protection (Registration and Licensing) Regulations, 2021 and the Data Protection (General) Regulations, 2024, together with relevant guidance, codes, standards, and compliance requirements issued by the Data Protection Commission. Where applicable to its operations, YPDP shall also comply with other Zambian legislation governing information, communications, cybersecurity, electronic transactions, employment, financial records, and the protection of specific categories of individuals or information.

In implementing this Policy, YPDP shall take into account applicable regulatory guidance and good practice relating to data protection, including requirements concerning the registration of data controllers and processors, data security, management of personal data breaches, records of processing activities, data protection training, and other compliance measures issued by the Data Protection Commission. Where there is any conflict between this Policy and applicable Zambian law or regulatory requirements, the applicable law or regulatory requirement shall prevail. This Policy shall be reviewed and updated as necessary to reflect changes in legislation, regulations, regulatory guidance, organisational operations, or data protection practices.

6. DATA PROTECTION PRINCIPLES

Youth Projects Development Platform (YPDP) shall ensure that all personal data is processed in accordance with the principles of data protection established under applicable Zambian law. These principles shall guide all activities involving the collection, use, storage, sharing, retention, and disposal of personal data.

Lawfulness, Fairness and Transparency: Personal data shall be processed lawfully, fairly, and transparently. YPDP shall ensure that individuals are appropriately informed about how and why their personal data is collected and processed and that processing is undertaken on a lawful basis.

Purpose Limitation: Personal data shall be collected for specified, explicit, and legitimate purposes and shall not be further processed in a manner incompatible with those purposes.

Data Minimisation: YPDP shall collect and process only personal data that is adequate, relevant, and limited to what is necessary for the purposes for which it is processed.

Accuracy: YPDP shall take reasonable steps to ensure that personal data is accurate, complete where necessary, and kept up to date. Where inaccurate personal data is identified, appropriate steps shall be taken to correct or rectify it without undue delay.

Storage Limitation: Personal data shall not be retained in an identifiable form for longer than is necessary for the purposes for which it was collected or processed, subject to applicable legal, regulatory, contractual, or legitimate organisational requirements for retention.

Integrity and Confidentiality: YPDP shall process personal data in a manner that ensures its security and confidentiality and shall implement appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing, loss, destruction, damage, alteration, or unauthorised disclosure.

Respect for Data Subject Rights: YPDP shall process personal data in accordance with the rights of data subjects as provided under applicable law. The organisation shall establish appropriate mechanisms for individuals to exercise their rights and raise concerns regarding the processing of their personal data.

Accountability: YPDP shall be responsible for demonstrating compliance with these data protection principles. The organisation shall maintain appropriate policies, procedures, records, safeguards, and other internal mechanisms necessary to demonstrate that personal data is processed responsibly and in accordance with applicable requirements.

7. PERSONAL DATA COLLECTED AND PROCESSED

In carrying out its programmes, projects, administrative functions, fundraising, communications, and other organisational activities, Youth Projects Development Platform may collect and process different categories of personal data. The nature and extent of personal data collected shall depend on the purpose for which it is required and shall be limited to information that is necessary and relevant to that purpose.

The categories of personal data that YPDP may collect and process include:

Identification and Contact Information

This may include names, residential or postal addresses, telephone numbers, email addresses, identification numbers, dates of birth, and other information necessary to identify or communicate with an individual.

Employee, Volunteer and Applicant Information

This may include information relating to employees, volunteers, interns, consultants, and job or programme applicants, including employment history, qualifications, references, contact details, identification information, and other information required for recruitment, engagement, and human resource management.

Beneficiary and Programme Participant Information

YPDP may collect information relating to beneficiaries and participants in its programmes and projects. This may include demographic information, community or organisational affiliation, participation records, needs assessments, programme activities, feedback, monitoring information, and other information necessary for programme implementation and reporting.

Donor and Funding Partner Information

This may include names, contact details, donation or funding information, correspondence, payment-related information, and records of interactions with donors and funding partners.

Partner and Service Provider Information

YPDP may collect information relating to partner organisations, consultants, contractors, suppliers, and service providers, including contact details, organisational information, contractual information, and correspondence.

Photographs, Audio and Video Recordings

YPDP may collect photographs, video recordings, audio recordings, and other visual or recorded material in connection with its programmes, events, communications, documentation, monitoring, reporting, and public awareness activities, subject to applicable consent and data protection requirements.

Financial and Transaction Information

Where necessary for legitimate organisational purposes, YPDP may process information relating to payments, donations, reimbursements, invoices, financial transactions, and other financial records. Access to such information shall be restricted to authorised persons and used only for legitimate purposes.

Website and Online Information

YPDP may collect information generated through its website, online forms, digital platforms, and other electronic services. This may include contact information, online identifiers, technical information, IP addresses, browser information, cookies, and information concerning interactions with its online services.

Correspondence and Communications

YPDP may retain records of communications and correspondence with individuals and organisations, including emails, letters, telephone records, enquiries, complaints, feedback, and other communications relating to its work.

Monitoring, Evaluation and Research Information

YPDP may collect and process information for monitoring, evaluation, learning, research, programme reporting, impact assessment, and organisational improvement. Where appropriate, information shall be aggregated, anonymised, or otherwise protected to minimise risks to individuals.

Sensitive Personal Data

Where necessary and permitted by applicable law, YPDP may process sensitive personal data, including information relating to health, biometric information, political opinions, religious or other beliefs, ethnic origin, sex, or information relating to child abuse or other categories recognised as sensitive under Zambian law. Such information shall be collected and processed only where there is a lawful basis and appropriate safeguards are in place.

YPDP shall not collect or process personal data merely because it may be useful. The organisation shall seek to ensure that personal data collected is relevant, adequate, accurate, and limited to what is necessary for the identified purpose. Where personal data is no longer required for the purpose for which it was collected, it shall be retained, archived, anonymised, or securely disposed of in accordance with this Policy and applicable legal requirements.

8. COLLECTION AND PROCESSING OF PERSONAL DATA

YPDP shall collect and process personal data only for lawful, specific, and legitimate purposes and in accordance with the principles established under this Policy and applicable Zambian data protection requirements.

Methods of Collection

YPDP may collect personal data directly from individuals through:

- Programme and project registration or participation forms;
- Employment, volunteer, internship, and consultancy applications;
- Membership or stakeholder registration;
- Donor and fundraising activities;
- Surveys, assessments, interviews, and monitoring and evaluation activities;
- Meetings, workshops, training sessions, events, and other organisational activities;
- Telephone calls, emails, letters, and other correspondence;
- The YPDP website, online forms, and other digital platforms; and
- Other legitimate interactions with the organisation.

YPDP may also receive personal data from third parties, including programme partners, funding partners, service providers, authorised representatives, or publicly available sources, where such collection is permitted by applicable law and does not unjustifiably prejudice the rights or interests of the data subject.

Direct Collection

YPDP shall, as a general rule, collect personal data directly from the data subject. Where personal data is collected directly, YPDP shall provide appropriate information about the organisation, the purpose of collection, the intended use of the data, and other information required under applicable law.

Collection from Other Sources

Where YPDP collects personal data from a source other than the data subject, it shall ensure that there is a lawful basis for doing so. Such collection may occur where the information is publicly available, the data subject has consented, collection from another source is permitted or required by law, or another circumstance recognised under applicable law applies.

Processing of Personal Data

YPDP shall process personal data only for purposes that are lawful, specific, legitimate, and compatible with the purpose for which the information was collected. Processing may include recording, organising, storing, retrieving, consulting, using, sharing, updating, transmitting, anonymising, archiving, or securely destroying personal data.

YPDP shall limit the collection and processing of personal data to information that is adequate, relevant, and necessary for the identified purpose. Personal data shall not be collected or processed merely because it may be useful in the future.

Consent and Other Lawful Grounds

Where consent is the lawful basis for processing, YPDP shall obtain consent in an informed, specific, freely given, and unambiguous manner and shall maintain appropriate evidence of such consent. Individuals shall be informed of their right to withdraw consent where processing is based on consent.

Where applicable, YPDP may process personal data on other lawful grounds recognised under the Data Protection Act, including where processing is necessary for the performance of a contract, compliance with a legal obligation, protection of vital interests, performance of a task carried out in the public interest, or legitimate interests, subject to the requirements and safeguards provided by law.

Accuracy and Updating of Information

YPDP shall take reasonable steps to ensure that personal data collected and processed is accurate, complete where necessary, and kept up to date. Individuals may be requested to provide updated information where necessary to ensure the accuracy and integrity of organisational records.

Collection of Sensitive Personal Data

YPDP shall only collect and process sensitive personal data where such processing is permitted by applicable law and appropriate safeguards are in place. Access to sensitive personal data shall be restricted to authorised persons who require the information for legitimate organisational purposes.

Collection of Children's and Vulnerable Persons' Data

Where YPDP's programmes involve children or vulnerable persons, the organisation shall apply appropriate safeguards when collecting and processing their personal data. Consent and other requirements applicable to children and vulnerable persons shall be observed in accordance with applicable Zambian law.

Unsolicited Personal Data

Where YPDP receives personal data that it did not intentionally request or collect, the organisation shall assess whether the information may lawfully be retained and processed. Where retention or processing is not justified, YPDP shall take appropriate steps to securely delete, destroy, or anonymise the information, subject to applicable legal or organisational requirements.

9. LAWFUL BASIS FOR PROCESSING

Youth Projects Development Platform shall process personal data only where there is a lawful basis for doing so in accordance with the Data Protection Act No. 3 of 2021 and other applicable legal requirements. Before processing personal data, YPDP shall identify and document the applicable lawful basis for the processing.

The lawful bases that may apply to YPDP's activities include:

- a. **Consent:** YPDP may process personal data where the data subject has given informed, specific, freely given, and unambiguous consent to the processing. Where processing is based on consent, YPDP shall maintain appropriate evidence of that consent and inform the data subject of the right to withdraw consent.
- b. **Performance of a Contract:** YPDP may process personal data where processing is necessary for the performance of a contract to which the data subject is a party, or to take steps at the request of the data subject before entering into a contract.
- c. **Compliance with a Legal Obligation:** YPDP may process personal data where processing is necessary to comply with a legal obligation to which the organisation is subject, including applicable statutory, regulatory, employment, financial, accounting, or reporting requirements.
- d. **Protection of Vital Interests:** YPDP may process personal data where processing is necessary to protect the vital interests of the data subject or another natural person, particularly in circumstances involving an emergency or serious threat to life or safety.

- e. **Public Interest:** YPDP may process personal data where processing is necessary for the performance of a task carried out in the public interest, where such processing is permitted under applicable law.
- f. **Legitimate Interests:** YPDP may process personal data where processing is necessary for the legitimate interests pursued by YPDP or a third party, provided that those interests do not override the fundamental rights and freedoms of the data subject. Particular care shall be taken where the data subject is a child or otherwise requires enhanced protection.
- g. **Personal Data Made Public by the Data Subject:** YPDP may process personal data where the data subject has intentionally and manifestly made the information public, subject to the requirements and limitations established under applicable law.
- h. **Sensitive Personal Data:** YPDP shall apply additional safeguards when processing sensitive personal data. Such data shall only be processed where the conditions permitted under the Data Protection Act and other applicable laws have been satisfied.
- i. **Documentation of Lawful Basis:** YPDP shall, where appropriate, document the lawful basis relied upon for processing personal data and ensure that the basis is appropriate to the purpose and circumstances of the processing. Where the lawful basis for processing changes, YPDP shall review and update its records and, where necessary, provide appropriate information to the affected data subjects.

No personal data shall be processed where YPDP cannot establish a lawful and legitimate basis for the processing.

10. CONSENT AND WITHDRAWAL OF CONSENT

Youth Projects Development Platform (YPDP) shall obtain and manage consent in a manner that is lawful, informed, transparent, and consistent with the requirements of the Data Protection Act No. 3 of 2021. Where consent is relied upon as the lawful basis for processing personal data, YPDP shall ensure that the consent is freely given, specific, informed, and unambiguous.

Obtaining Consent

Where consent is required, YPDP shall:

- a. Clearly explain the purpose for which personal data will be collected and processed;
- b. Provide sufficient information to enable the data subject to make an informed decision;
- c. Obtain consent through a clear affirmative action or written declaration, where appropriate;

- d. Ensure that consent is distinguishable from other matters and presented in clear and accessible language; and
- e. Avoid making the provision of services or participation in activities conditional on consent where the processing is not necessary for that service or activity.

Recording and Evidence of Consent

YPDP shall maintain appropriate records demonstrating that consent was obtained where processing is based on consent. Records may include signed consent forms, electronic confirmations, registration records, or other appropriate evidence. The record of consent should, where applicable, indicate the identity of the data subject, the purpose of processing, the date consent was provided, and the manner in which consent was obtained.

Withdrawal of Consent

A data subject has the right to withdraw consent at any time where processing is based on consent. YPDP shall provide a reasonable and accessible means through which consent may be withdrawn.

Withdrawal of consent shall not affect the lawfulness of processing carried out before the withdrawal. Following withdrawal, YPDP shall cease processing the relevant personal data where there is no other lawful basis for continuing the processing and shall take appropriate steps regarding the retention or destruction of the data in accordance with applicable law and this Policy.

Consent for Communications

Where YPDP relies on consent to send newsletters, promotional communications, event information, fundraising communications, or other optional communications, individuals shall be given a clear opportunity to opt in and, where applicable, to withdraw their consent or unsubscribe from such communications.

Consent for Photographs, Audio and Video

Where YPDP intends to use identifiable photographs, audio recordings, video recordings, or similar materials for purposes requiring consent, the organisation shall obtain appropriate consent from the individual before such use, unless another lawful basis applies.

The consent process shall, where appropriate, explain how the material will be used, the intended audience or publication channels, and the purpose for which it will be used.

Consent Involving Children and Vulnerable Persons

Where personal data relating to a child or vulnerable person is processed on the basis of consent, YPDP shall comply with the additional requirements under applicable Zambian law and shall take appropriate steps to verify consent from the parent, legal guardian, or person exercising parental responsibility, where required.

Review of Consent

YPDP shall periodically review consent where the purpose or manner of processing changes. Where a new purpose is materially different from the purpose for which consent was originally obtained and no other lawful basis applies, YPDP shall obtain appropriate consent before undertaking the new processing.

11. USE AND DISCLOSURE OF PERSONAL DATA

Youth Projects Development Platform shall use and disclose personal data only for lawful, specific, and legitimate purposes and in accordance with the applicable lawful basis, this Policy, and the Data Protection Act No. 3 of 2021.

Use of Personal Data

YPDP may use personal data for purposes that are necessary for the effective and legitimate operation of the organisation, including:

- a. Implementing and managing programmes and projects;
- b. Communicating with beneficiaries, participants, members, staff, volunteers, donors, partners, and other stakeholders;
- c. Managing employment, volunteer, consultancy, and other organisational relationships;
- d. Processing donations, payments, reimbursements, and other legitimate financial transactions;
- e. Monitoring, evaluation, research, learning, reporting, and organisational improvement;
- f. Fulfilling contractual, legal, regulatory, accounting, and reporting obligations;
- g. Organising meetings, workshops, training, events, and other organisational activities;
- h. Managing complaints, enquiries, safeguarding concerns, and other matters requiring organisational action;
- i. Maintaining organisational records and ensuring accountability to relevant stakeholders; and
- j. Preventing, detecting, and responding to fraud, misuse, security incidents, or other unlawful activities.

YPDP shall not use personal data for a new or incompatible purpose unless such processing is permitted by law or the organisation has obtained the necessary consent or established another lawful basis for the processing.

Disclosure of Personal Data

YPDP shall not disclose personal data to another person or organisation unless the disclosure is lawful and necessary for a legitimate and identified purpose. Where consent is required for disclosure, YPDP shall obtain the consent of the data subject before the disclosure. Where personal data is to be disclosed, YPDP shall, where required by law, inform the data subject of:

- a. When and to whom the information will be disclosed;
- b. The purpose of the disclosure;
- c. The measures and policies in place to protect the information; and
- d. The available procedure for raising a concern or seeking recourse regarding the disclosure.

Permitted Recipients

Subject to applicable law and the relevant lawful basis, YPDP may disclose personal data to authorised:

- a. Programme and implementation partners;
- b. Donors and funding partners, where necessary for legitimate reporting or accountability purposes;
- c. Consultants, contractors, and service providers;
- d. Auditors, accountants, lawyers, and other professional advisers;
- e. Financial institutions and payment service providers;
- f. Government authorities and regulatory bodies where required or authorised by law; and
- g. Other persons or organisations where the disclosure is lawful, necessary, and appropriately safeguarded.

YPDP shall limit information disclosed to third parties to the minimum information reasonably necessary for the stated purpose.

Disclosure to Data Processors

Where YPDP engages a data processor to process personal data on its behalf, the relationship shall be governed by an appropriate written agreement setting out the purpose and nature of processing, the categories of personal data and data subjects involved, and the respective obligations and responsibilities of the parties.

YPDP shall take reasonable steps to ensure that data processors implement appropriate measures to protect personal data and process it only in accordance with authorised instructions and applicable law.

Disclosure Required by Law

YPDP may disclose personal data where disclosure is required or authorised by applicable law, including where necessary for the fulfilment of a legal obligation or for purposes permitted under the Data Protection Act.

Where legally permitted, YPDP shall take reasonable steps to inform the affected data subject of such disclosure.

Public Disclosure and Communications

YPDP shall exercise particular caution when publishing personal data through its website, social media platforms, annual reports, newsletters, publications, photographs, videos, or other public communications.

Personal data shall not be publicly disclosed merely because it is available within the organisation. YPDP shall ensure that any public disclosure has an appropriate lawful basis and is consistent with the purpose for which the information was collected.

Confidentiality and Need-to-Know Access

Access to personal data within YPDP shall be limited to authorised persons who require the information to perform legitimate organisational responsibilities. Persons with access to personal data shall maintain confidentiality and shall not disclose or use the information for unauthorised purposes.

Records of Disclosure

YPDP shall maintain appropriate records of disclosures of personal data, including, where applicable, the information disclosed, the recipient, the purpose of disclosure, and the date of disclosure, in accordance with applicable legal and organisational requirements.

12. DATA SUBJECT RIGHTS

Youth Projects Development Platform (YPDP) recognises and respects the rights of individuals in relation to their personal data as provided under the Data Protection Act No. 3 of 2021 and other applicable laws. YPDP shall establish appropriate mechanisms to enable data subjects to exercise their rights and shall respond to legitimate requests within the timeframes prescribed by applicable law.

Right to Be Informed

A data subject has the right to receive clear and appropriate information about the collection and processing of their personal data, including the purposes of processing, the categories of data involved, the intended recipients, applicable retention periods, and their rights under the law.

Right of Access

A data subject has the right to request confirmation as to whether YPDP is processing their personal data and, where applicable, to access their personal data and relevant information concerning its processing.

Right to Rectification

A data subject has the right to request the correction or updating of personal data that is inaccurate, incomplete, or outdated. YPDP shall take reasonable steps to correct such information where the request is justified.

Right to Erasure

A data subject may request the deletion or erasure of their personal data where the conditions provided under applicable law are satisfied, including where the data is no longer necessary for the purpose for which it was collected, where consent has been withdrawn and no other lawful basis exists, or where the processing is unlawful. The right to erasure is subject to applicable legal and regulatory requirements, including circumstances in which YPDP may be required or permitted to retain information.

Right to Restriction of Processing

A data subject may, where permitted by law, request that the processing of their personal data be restricted in circumstances where there is a dispute concerning the processing or the accuracy or lawfulness of the data. Where processing is restricted, YPDP shall comply with the applicable requirements concerning the use and storage of the restricted data.

Right to Data Portability

Where applicable, a data subject may request their personal data in a structured and commonly used format and may request that the data be transferred to another data controller, subject to the conditions and limitations established by law.

Right to Object to Processing

A data subject has the right to object to the processing of their personal data where permitted by law. YPDP shall consider such objections and shall cease or restrict processing where required, unless there are lawful grounds that permit or require the organisation to continue processing.

Right to Object to Direct Marketing

A data subject has the right to object to the processing of their personal data for direct marketing purposes. Where an individual objects to such processing, YPDP shall cease the relevant direct marketing processing in accordance with applicable law.

Rights Relating to Automated Decision-Making

Where applicable, a data subject has rights concerning decisions based solely on automated processing, including profiling, where such processing produces legal effects or similarly significant effects concerning the individual. YPDP shall comply with applicable safeguards and requirements governing such processing.

Right to Withdraw Consent

Where processing is based on consent, a data subject has the right to withdraw that consent at any time. Withdrawal shall not affect the lawfulness of processing carried out before the withdrawal.

Right to Lodge a Complaint

A data subject who believes that YPDP has processed their personal data unlawfully or has otherwise infringed their data protection rights may raise the matter with YPDP through the organisation's designated complaints or data protection contact.

Where the matter is not satisfactorily resolved, the data subject may exercise their right to lodge a complaint with the Data Protection Commission or pursue any other remedy available under applicable law.

Exercising Data Subject Rights

Requests concerning data subject rights shall be submitted through the contact mechanism designated by YPDP. YPDP may take reasonable steps to verify the identity of the person making a request before providing access to personal data or taking action on the request. YPDP shall assess and respond to requests in accordance with applicable legal requirements. Where a request cannot be granted, YPDP shall, where required by law, provide the data subject with the reason for the decision and information on available avenues for review or complaint.

13. DATA SHARING AND THIRD PARTIES

YPDP may share personal data with third parties where such sharing is necessary for a legitimate organisational purpose, permitted by applicable law, and supported by an appropriate lawful basis. YPDP shall ensure that personal data shared with third parties is limited to what is necessary for the intended purpose and is subject to appropriate safeguards.

Categories of Third Parties

Depending on the nature of its activities, YPDP may share personal data with:

- a. Donors and funding partners, where necessary for programme implementation, monitoring, evaluation, accountability, or reporting;
- b. Implementing and programme partners involved in delivering ydpd activities;
- c. Consultants, contractors, and professional advisers engaged by ydpd;
- d. Service providers that provide information technology, communications, financial, administrative, monitoring, or other services;
- e. Auditors, accountants, lawyers, and other professional advisers;
- f. Banks, payment service providers, and other financial institutions where necessary for legitimate financial transactions;
- g. Government ministries, departments, agencies, regulators, or law enforcement authorities where disclosure is required or authorised by law; and
- h. Other legitimate recipients where sharing is necessary, lawful, and consistent with this policy.

Conditions for Sharing

Before sharing personal data with a third party, YPDP shall, where appropriate:

- a. establish the lawful basis for the sharing;
- b. identify the purpose and necessity of the disclosure;
- c. limit the information shared to what is adequate, relevant, and necessary;
- d. consider the sensitivity and potential risks associated with the information;
- e. ensure that appropriate confidentiality and security safeguards are in place; and
- f. provide the data subject with appropriate information about the sharing where required by law.

Third-Party Service Providers and Data Processors

Where a third party processes personal data on behalf of YPDP, the third party shall be appropriately assessed and engaged under a written agreement or other legally enforceable arrangement where required.

The agreement shall, where applicable, define the purpose and nature of processing, the categories of personal data and data subjects involved, the duration of processing, and the responsibilities of the parties.

Third-party processors shall be required to process personal data only for authorised purposes, maintain confidentiality, implement appropriate security measures, and comply with applicable data protection requirements.

Donors and Funding Partners

Where donors or funding partners require personal data for legitimate programme, monitoring, evaluation, safeguarding, accountability, or reporting purposes, YPDP shall share only the information reasonably necessary to meet the requirement. Where possible and appropriate, YPDP shall use aggregated, anonymised, or pseudonymised information when individual identification is not necessary.

Implementing Partners

Where personal data needs to be shared with implementing or programme partners, YPDP shall ensure that the partner understands and accepts its data protection responsibilities. The partner shall use the information only for the agreed purpose and shall implement appropriate measures to protect it from unauthorised access, disclosure, loss, misuse, alteration, or destruction.

Disclosure to Government and Other Authorities

YPDP may disclose personal data to government authorities, regulators, law enforcement agencies, courts, or other competent authorities where required or authorised by law. Where legally permitted, YPDP shall take reasonable steps to ensure that such requests are legitimate and that only the information necessary to satisfy the lawful request is disclosed.

Confidentiality

All third parties who are authorised to access personal data on behalf of YPDP shall be required to maintain the confidentiality of that information. Access to personal data shall be restricted to individuals who have a legitimate need to access it for the authorised purpose.

International or Cross-Border Sharing

YPDP shall apply appropriate safeguards where personal data is transferred or made accessible outside Zambia. Such transfers shall only take place where the requirements of applicable Zambian data protection law have been satisfied.

Third-Party Compliance

YPDP shall take reasonable steps to assess whether third parties with access to personal data have appropriate privacy and security practices. Where a third party fails to comply with applicable data protection requirements or the terms of its agreement with YPDP, the organisation shall take appropriate corrective action, which may include restricting access, requiring remedial measures, or terminating the arrangement.

Records of Data Sharing

YPDP shall maintain appropriate records of significant or recurring disclosures of personal data, including the recipient, purpose, categories of information shared, and relevant safeguards, where required by law or organisational procedures.

14. CROSS-BORDER/INTERNATIONAL DATA TRANSFERS

Youth Projects Development Platform recognises that personal data may, in certain circumstances, need to be accessed, processed, stored, or transferred outside Zambia in connection with international partnerships, donor requirements, consultancy arrangements, technology services, cloud-based systems, or other legitimate organisational activities.

YPDP shall ensure that any cross-border transfer of personal data is undertaken in accordance with the Data Protection Act No. 3 of 2021 and applicable regulations, requirements, and guidance issued by the Data Protection Commission.

General Requirements

YPDP shall not transfer personal data outside Zambia unless the transfer is lawful and the applicable requirements for cross-border transfers have been satisfied.

Before undertaking a cross-border transfer, YPDP shall assess:

- a. The purpose and necessity of the transfer;
- b. The categories and sensitivity of the personal data involved;
- c. The recipient and the country or jurisdiction to which the data will be transferred;
- d. The safeguards applicable to the transfer;
- e. Whether the transfer is permitted under zambian law; and
- f. The potential risks to the rights and freedoms of the affected data subjects.

International Donors and Partners

Where YPDP needs to share personal data with an international donor, implementing partner, consultant, service provider, or other organisation located outside Zambia, the organisation shall ensure that the transfer has an appropriate lawful basis and complies with the requirements applicable to cross-border transfers.

Where individual-level information is not necessary, YPDP shall, where reasonably practicable, use aggregated, anonymised, or pseudonymised information instead of identifiable personal data.

Cloud-Based and Technology Services

YPDP shall take reasonable steps to determine where personal data is stored and processed when using cloud-based platforms, software, online databases, email systems, file-sharing services, or other technology services.

Where such services involve the storage or processing of personal data outside Zambia, YPDP shall ensure that the applicable requirements for cross-border transfers are satisfied and that appropriate contractual, technical, and organisational safeguards are in place.

Sensitive Personal Data

YPDP shall apply particular caution to any proposed transfer of sensitive personal data outside Zambia. Sensitive personal data shall be processed and stored in Zambia in accordance with the requirements of the Data Protection Act. Any permitted transfer of sensitive personal data outside Zambia shall comply with the specific conditions established by applicable law, including any requirement for explicit consent or other lawful authorisation.

Safeguards for International Transfers

Where a cross-border transfer is permitted, YPDP shall use appropriate safeguards required or recognised under Zambian law. Depending on the circumstances, these may include:

- a. Approved standard contractual clauses;
- b. Approved binding or intragroup arrangements, where applicable;
- c. Transfer to a jurisdiction recognised as providing an adequate level of protection;
- d. Approval or authorisation from the data protection commission where required; or
- e. Another lawful exception or mechanism recognised under applicable law.

International Service Providers and Processors

Where an international organisation processes personal data on behalf of YPDP, YPDP shall ensure that the relationship is governed by an appropriate written agreement and that the processor is subject to appropriate confidentiality, security, data protection, and cross-border transfer obligations. YPDP shall take reasonable steps to ensure that the processor does not transfer the personal data to another country or third party except where such further transfer is lawful and appropriately safeguarded.

Information to Data Subjects

Where required by applicable law, YPDP shall inform data subjects that their personal data may be transferred outside Zambia and provide relevant information concerning the destination, purpose of the transfer, and safeguards applied to protect their personal data.

Records of Cross-Border Transfers

YPDP shall maintain appropriate records of significant or recurring international transfers of personal data, including the recipient, purpose, categories of personal data transferred, destination, lawful basis, applicable safeguards, and any relevant approval or authorisation.

Review of International Arrangements

YPDP shall periodically review international data-sharing and processing arrangements to ensure that they remain lawful and that the safeguards protecting personal data remain appropriate.

Where a transfer arrangement no longer satisfies applicable legal or organisational requirements, YPDP shall take appropriate corrective action, which may include suspending the transfer, changing the service provider, strengthening safeguards, or terminating the arrangement.

15. DATA SECURITY AND CONFIDENTIALITY

Youth Projects Development Platform shall take appropriate technical, organisational, administrative, and physical measures to protect personal data against unauthorised or unlawful processing, access, disclosure, alteration, loss, destruction, misuse, or damage. The security measures applied by YPDP shall be proportionate to the nature, sensitivity, volume, and risks associated with the personal data being processed and shall be reviewed periodically.

Physical Security

YPDP shall take reasonable measures to protect physical records, devices, offices, and other locations where personal data is stored or accessed. Such measures may include:

- a. Securing offices, filing cabinets, storage rooms, and other areas containing personal data;
- b. Restricting access to areas containing sensitive or confidential information;
- c. Ensuring that paper records are not left unattended or exposed to unauthorised persons;
- d. Protecting computers, servers, storage devices, and other equipment from theft, damage, or unauthorised access; and
- e. Maintaining appropriate arrangements for the secure disposal of physical records.

Electronic and Technical Security

YPDP shall implement appropriate technical safeguards to protect electronic personal data, including, where appropriate:

- a. Password protection and user authentication;
- b. Access controls and user permissions;
- c. Encryption of personal data where appropriate;
- d. Secure storage and transmission of personal data;
- e. Protection against malware, viruses, and other security threats;

- f. Regular software and security updates;
- g. Secure configuration of devices and information systems; and
- h. Appropriate monitoring and security measures to identify unauthorised access or suspicious activity.

Access Controls

Access to personal data shall be granted on a need-to-know and role-based basis. Personnel shall only have access to personal data that is necessary for the performance of their authorised responsibilities.

YPDP shall periodically review user access rights and shall promptly remove or modify access when an individual changes responsibilities, leaves the organisation, or no longer requires access to the information.

Passwords and Authentication

YPDP shall require appropriate password and authentication practices for systems containing personal data. Personnel shall:

- a. Use strong and appropriately managed passwords;
- b. Keep passwords confidential and not share them with other persons;
- c. Avoid using the same password across systems where this creates an unnecessary security risk;
- d. Use multi-factor authentication where available and appropriate; and
- e. Report suspected compromise of passwords or user accounts promptly.

Confidentiality Obligations

All Board members, employees, volunteers, interns, consultants, contractors, and other persons who have access to personal data on behalf of YPDP shall maintain the confidentiality of such information.

Personal data shall only be accessed, used, copied, disclosed, or discussed for authorised organisational purposes. Confidentiality obligations shall continue after an individual's employment, contract, volunteer engagement, or other relationship with YPDP ends, subject to applicable law.

Storage and Backups

YPDP shall store personal data using appropriate physical and electronic safeguards. Where personal data is stored electronically, appropriate backup arrangements shall be maintained to reduce the risk of permanent loss.

Backups containing personal data shall be protected against unauthorised access, alteration, loss, theft, or destruction and shall be retained only for as long as necessary.

Portable Devices and Remote Access

Where personal data is accessed or stored on laptops, mobile phones, removable storage devices, or other portable equipment, YPDP shall apply appropriate security measures to reduce the risk of loss, theft, or unauthorised access.

Remote access to organisational systems containing personal data shall be authorised and secured using appropriate authentication and technical safeguards.

Sharing and Transmission of Personal Data

Personal data shall only be transmitted through appropriate and reasonably secure channels. Personnel shall exercise particular care when sending personal data by email, messaging platforms, file-sharing services, or other electronic means. Where appropriate, sensitive personal data shall be encrypted or otherwise protected before transmission.

Data Breach and Security Incident Reporting

Any actual or suspected loss, theft, unauthorised access, disclosure, alteration, destruction, or other compromise of personal data shall be reported immediately to the person designated by YPDP to manage data protection matters.

YPDP shall maintain procedures for assessing, containing, investigating, documenting, and responding to personal data breaches and shall make notifications to the Data Protection Commission and affected data subjects within the timeframes required by applicable law. Under the Data Protection Act, a data controller is required to notify the Data Protection Commissioner within twenty-four hours of a security breach affecting personal data, while a data processor must notify the controller as soon as practicable.

Third-Party Security

Where YPDP engages a third party to process or store personal data, the organisation shall take reasonable steps to ensure that the third party provides appropriate technical and organisational safeguards. Relevant contractual arrangements shall include appropriate confidentiality, security, data protection, breach notification, and data handling obligations.

Security Awareness and Training

YPDP shall promote awareness of data protection and information security among persons who process or have access to personal data on its behalf. Appropriate personnel shall receive training or guidance on confidentiality, secure handling of personal data, password security, phishing and other common threats, breach reporting, and their responsibilities under this Policy.

Periodic Review of Security Measures

YPDP shall periodically review its technical and organisational security measures to determine whether they remain appropriate to the risks associated with its processing activities. Where weaknesses or emerging risks are identified, YPDP shall take reasonable steps to strengthen its safeguards and reduce the likelihood or impact of a personal data breach.

16. DATA RETENTION, ARCHIVING AND DISPOSAL

YPDP shall retain personal data only for as long as it is necessary to fulfil the purpose for which it was collected or processed, or for as long as retention is required or permitted by applicable law, contractual obligations, legitimate organisational requirements, or other lawful purposes. The Organization shall seek to balance the legitimate need to retain information for accountability, programme delivery, organisational learning, legal compliance, and institutional record keeping with the need to avoid retaining personal data unnecessarily.

Retention Principles

YPDP shall:

- a. Identify the purpose for which personal data is being retained;
- b. Determine an appropriate retention period based on the nature and purpose of the information;
- c. Consider applicable legal, regulatory, contractual, donor, financial, audit, safeguarding, and organisational requirements;
- d. Avoid retaining personal data for longer than is necessary;

- e. periodically review retained personal data to determine whether it is still required; and
- f. securely dispose of or anonymise personal data when it is no longer required, subject to applicable retention requirements.

Retention Periods

Retention periods shall vary according to the type and purpose of personal data. YPDP shall, where appropriate, establish and maintain a records retention schedule identifying the categories of records, applicable retention periods, responsible persons, and approved disposal methods. Examples of information that may require different retention considerations include:

- a. Employee and human resource records;
- b. Beneficiary and programme participant records;
- c. Donor and fundraising records;
- d. Financial and accounting records;
- e. Monitoring, evaluation, and research records;
- f. Contractual and partner records;
- g. Photographs, audio, and video recordings;
- h. Correspondence and complaints;
- i. Safeguarding and incident records; and
- j. Website and digital records.

Where a specific retention period is prescribed by law, regulation, contract, donor requirement, or another binding obligation, YPDP shall comply with the applicable requirement.

Archiving

Certain records may need to be retained beyond their immediate operational use because of their historical, legal, institutional, accountability, research, or organisational value. Where personal data is archived, YPDP shall ensure that:

- a. access is limited to authorised persons;
- b. the information remains appropriately protected;
- c. the purpose for continued retention is documented;
- d. archived information is not routinely used for unrelated purposes; and
- e. the information is reviewed periodically to determine whether continued retention remains justified.

Where appropriate, personal data may be anonymised before being retained for historical, research, statistical, or organisational learning purposes.

Suspension of Disposal

Where personal data is relevant to an actual or anticipated investigation, audit, legal proceeding, complaint, safeguarding matter, regulatory inquiry, or other legitimate organisational process, YPDP may suspend routine disposal of the relevant records until the matter has been concluded or disposal is otherwise authorised.

Secure Disposal

When personal data is no longer required and there is no lawful reason to retain it, YPDP shall ensure that it is securely disposed of, deleted, or anonymised. Depending on the format and circumstances, secure disposal may include:

- a. Shredding or securely destroying paper records;
- b. Securely deleting electronic files;
- c. Permanently removing information from appropriate storage systems;
- d. Securely wiping or destroying electronic storage devices; and
- e. Using appropriate procedures to prevent discarded records or equipment from being used to recover personal data.

Disposal by Third Parties

Where a third party holds or processes personal data on behalf of YPDP, the organisation shall ensure that contractual arrangements address the return, deletion, destruction, or continued retention of personal data when the relevant service or processing relationship ends. YPDP shall take reasonable steps to ensure that third parties securely dispose of personal data in accordance with agreed requirements and applicable law.

Anonymisation

Where information has continuing statistical, research, monitoring, evaluation, historical, or organisational value but identifiable personal data is no longer required, YPDP may anonymise the information rather than retain it in an identifiable form. Anonymised information shall be handled in a manner that prevents individuals from being reasonably identified from the information.

Responsibility for Retention and Disposal

The person responsible for managing a particular record or information system shall ensure that personal data is retained, archived, reviewed, and disposed of in accordance with this Policy and any applicable records retention schedule or organisational procedure. Managers and relevant personnel shall cooperate in periodic reviews of records to identify information that is no longer required.

Periodic Review

YPDP shall periodically review its retention practices to ensure that personal data is not retained unnecessarily and that retention periods remain appropriate to the organisation's legal, operational, contractual, and programme requirements.

17. DATA BREACH MANAGEMENT

Youth Projects Development Platform (YPDP) shall maintain appropriate procedures for identifying, reporting, assessing, containing, managing, documenting, and responding to personal data breaches.

A personal data breach includes any actual or suspected incident involving the unauthorised or unlawful access to, acquisition, disclosure, alteration, loss, destruction, or other compromise of personal data that may affect its confidentiality, integrity, or availability.

YPDP shall respond to data breaches promptly and in accordance with the Data Protection Act No. 3 of 2021 and applicable guidance issued by the Data Protection Commission.

Identification of a Data Breach

A data breach may arise from accidental, unlawful, deliberate, or malicious actions and may involve:

- a. Unauthorised access to personal data;
- b. Accidental disclosure or transmission of personal data to an unintended recipient;
- c. Loss or theft of files, computers, phones, storage devices, or other equipment containing personal data;
- d. Unauthorised alteration or destruction of personal data;
- e. Compromised user accounts, passwords, or information systems;

- f. Malware, phishing, hacking, or other cyber incidents;
- g. Inappropriate access or use of personal data by staff, volunteers, contractors, partners, or other authorised persons; or
- h. Any other incident that compromises the confidentiality, integrity, or availability of personal data.

Actual or suspected breaches shall be treated seriously and reported without delay.

Internal Reporting

Any Board member, employee, volunteer, consultant, contractor, partner, or other person who becomes aware of or suspects a personal data breach shall report the incident immediately to the person designated by YPDP to manage data protection matters. Personnel shall not delay reporting while attempting to determine whether an incident constitutes a breach. Initial reporting should, where possible, include:

- a. The date and time the incident was identified;
- b. A description of what happened;
- c. The systems, records, or information involved;
- d. The categories of personal data potentially affected;
- e. The persons or groups potentially affected;
- f. The person or organisation believed to be responsible, where known; and
- g. Any immediate action already taken.

Initial Assessment

Upon receiving a breach report, the responsible person shall conduct or coordinate an initial assessment to determine:

- a. Whether personal data is involved;
- b. The nature and extent of the breach;
- c. The categories and approximate amount of personal data affected;
- d. The number and categories of data subjects potentially affected;
- e. Whether sensitive personal data or information relating to children or vulnerable persons is involved;
- f. The likely consequences and potential harm to affected individuals;

- g. Whether the breach is ongoing;
- h. Whether third parties or data processors are involved; and
- i. Whether notification or other regulatory action is required.

The assessment shall be documented and updated as further information becomes available.

Containment and Immediate Response

YPDP shall take immediate and proportionate measures to contain the breach and prevent further unauthorised access, disclosure, loss, alteration, or destruction of personal data. Depending on the circumstances, containment measures may include:

- a. Disabling or restricting compromised user accounts;
- b. Changing passwords or access credentials;
- c. Isolating affected devices, systems, or networks;
- d. Recovering or securing lost equipment or records;
- e. Recalling information sent to an unintended recipient where practicable;
- f. Restricting further access to affected records;
- g. Correcting or restoring compromised information; and
- h. Engaging relevant technical, legal, security, or other professional support.

Evidence relating to the incident shall be preserved where necessary for investigation, regulatory reporting, legal proceedings, or other legitimate purposes.

Notification to the Data Protection Commission

Where YPDP is acting as a data controller, it shall notify the Data Protection Commissioner within the period required by the Data Protection Act. In particular, Section 49 of the Act requires a data controller to notify the Data Protection Commissioner within twenty-four hours of any security breach affecting personal data processed.

Where YPDP is acting as a data processor, it shall notify the relevant data controller as soon as practicable after becoming aware of a security breach affecting personal data processed on behalf of that controller.

YPDP shall maintain appropriate records of notifications made to the Data Protection Commission and other relevant parties.

Notification to Data Subjects

Where required by applicable law, YPDP shall notify affected data subjects as soon as practicable following a personal data breach. The notification shall, where appropriate, explain:

- a. The nature of the breach;
- b. The categories of personal data affected;
- c. The potential consequences of the breach;
- d. The measures ydpd has taken or proposes to take to address the breach;
- e. Steps the affected individual may take to reduce potential harm; and
- f. How the individual may obtain further information or raise concerns.

The form and timing of notification shall take into account the circumstances of the incident and applicable legal requirements.

Communication with Third Parties

Where a breach involves a data processor, implementing partner, service provider, donor, technology provider, or other third party, YPDP shall coordinate with the relevant party to investigate and contain the incident and to fulfil applicable notification and reporting obligations. Third parties processing personal data on behalf of YPDP shall be required to notify YPDP of suspected or confirmed breaches as soon as practicable and to provide reasonable assistance in investigating, containing, documenting, and resolving the incident.

Data Breach Register

YPDP shall maintain a data breach register or other appropriate record of actual and suspected personal data breaches. The record should, where applicable, include:

the date and time of the incident and its discovery;

- a. The nature and circumstances of the breach;
- b. The categories of personal data affected;
- c. The categories and approximate number of data subjects affected;
- d. The likely consequences of the breach;
- e. The actions taken to contain and address the incident;
- f. Notifications made to the data protection commission, data subjects, or other parties;
- g. Remedial and preventive measures implemented; and
- h. The date and outcome of the post-incident review.

The register shall be kept securely and retained in accordance with applicable legal and organisational requirements.

Corrective and Preventive Action

Following a breach, YPDP shall identify and implement appropriate corrective measures to address the cause of the incident and reduce the likelihood of recurrence. Corrective measures may include:

- a. Strengthening technical or physical security controls;
- b. Changing access permissions;
- c. Updating procedures or systems;
- d. Improving contractual safeguards with third parties;
- e. Additional staff or volunteer training;
- f. Reviewing data collection, retention, or sharing practices;
- g. Implementing additional monitoring or security measures; and
- h. Taking disciplinary, contractual, or other appropriate action where misconduct or negligence contributed to the breach.

Post-Incident Review

YPDP shall conduct a post-incident review following significant personal data breaches to determine:

- a. What happened and why;
- b. Whether the response was timely and effective;
- c. Whether notification requirements were properly addressed;
- d. Whether existing policies, procedures, or safeguards were adequate;
- e. What lessons can be learned; and
- f. What further improvements are required.

The findings of the review shall be documented and used to strengthen YPDP's data protection and information security practices.

Cooperation with the Data Protection Commission

YPDP shall cooperate with the Data Protection Commission and other competent authorities in relation to investigations, notifications, audits, or other lawful requirements arising from a personal data breach. YPDP shall provide information and assistance as required by applicable law and shall implement any lawful corrective measures or directions issued by the relevant authority.

18. ROLES AND RESPONSIBILITIES

Effective data protection is a shared responsibility within YPDP. The Board, management, employees, volunteers, consultants, contractors, programme teams, and third parties who process personal data on behalf of YPDP shall comply with this Policy and applicable data protection requirements. The following responsibilities shall apply:

The Board

The Board shall provide overall governance and oversight of data protection within YPDP and shall:

- a. Approve and periodically review this Policy;
- b. Provide appropriate oversight of the organisation's data protection and privacy arrangements;
- c. Ensure that management has appropriate resources and arrangements to protect personal data;
- d. Receive reports on significant data protection risks, breaches, compliance issues, and corrective actions; and
- e. Promote a culture of accountability, confidentiality, and responsible handling of personal data.

The Executive

Executive Management shall be responsible for implementing this Policy and ensuring that data protection requirements are integrated into YPDP's operations. Management shall:
ensure that appropriate procedures, controls, and resources are established;

- a. Ensure that staff and other relevant persons understand their data protection responsibilities;
- b. Oversee significant data protection risks and compliance matters;
- c. Ensure that appropriate action is taken following data breaches or other incidents;
- d. Support the designated data protection officer or responsible person in carrying out their responsibilities; and
- e. Ensure that material data protection issues are escalated to the Board where appropriate.

Data Protection Officer or Responsible Person

YPDP shall designate a Data Protection Officer or other suitably responsible person to coordinate the organisation's data protection activities, taking into account the requirements applicable to the organisation under Zambian law. The designated person shall, as appropriate:

- a. Advise management and personnel on their responsibilities under this Policy and applicable data protection requirements;
- b. Coordinate implementation of this Policy;
- c. Support the organisation in identifying and managing data protection risks;
- d. Coordinate responses to data subject requests and complaints;
- e. Support data breach assessment, reporting, investigation, and follow-up;
- f. Maintain or coordinate relevant data protection records and registers;
- g. Support privacy and data protection assessments for new projects, systems, or activities;
- h. Coordinate relevant engagement with the Data Protection Commission;
- i. Promote data protection awareness and training; and
- j. Report significant data protection risks or compliance concerns to management.

The designated person shall have sufficient authority and access to relevant information to perform these responsibilities effectively.

ICT and Systems

The ICT or systems function, or the person responsible for ICT where YPDP does not maintain a dedicated ICT department, shall support the implementation of appropriate technical safeguards. Responsibilities shall include:

- a. Implementing appropriate access controls and authentication measures;
- b. Supporting secure storage, transmission, backup, and recovery of electronic personal data;
- c. Maintaining appropriate security updates and system protections;
- d. Supporting the detection, containment, and investigation of information security incidents;
- e. Assisting with the secure disposal of electronic data and equipment;
- f. Supporting appropriate controls for remote access and portable devices; and
- g. Advising management on significant technology-related data protection and security risks.

Human Resources

Human Resources, or the person responsible for HR functions, shall ensure that personal data relating to employees, applicants, volunteers, interns, and other personnel is handled appropriately.

Responsibilities shall include:

- a. Collecting and processing personnel information only for legitimate purposes;
- b. Maintaining appropriate confidentiality and access controls;
- c. Ensuring that personnel are informed of relevant privacy and data protection requirements;
- d. Incorporating appropriate confidentiality and data protection obligations into employment or engagement arrangements where applicable;
- e. Supporting data protection awareness and training; and
- f. Ensuring that access to organisational information is reviewed when personnel join, change roles, or leave YPDP.

Programme and Project Teams

Programme and project teams shall ensure that personal data collected or processed through YPDP programmes is handled responsibly and only for authorised purposes. They shall:

- a. Collect only the personal data necessary for programme activities;
- b. Provide appropriate information to participants and beneficiaries;
- c. Obtain consent where consent is the applicable lawful basis;
- d. Protect beneficiary and participant information from unauthorised access or disclosure;
- e. Use appropriate safeguards when handling information relating to children or vulnerable persons;
- f. Ensure that personal data shared with programme partners is appropriately authorised and safeguarded;
- g. Promptly report suspected data breaches or inappropriate disclosures; and
- h. Comply with applicable retention and disposal requirements.

Finance and Administration

Finance and Administration shall ensure that personal and financial information is appropriately protected when performing financial and administrative functions. Responsibilities shall include:

- a. Securely handling donor, supplier, employee, consultant, and other financial information;
- b. Applying appropriate access controls to financial records;

- c. Ensuring that personal data contained in financial records is disclosed only for legitimate and authorised purposes;
- d. Supporting compliance with applicable financial, accounting, audit, and legal retention requirements; and
- e. Securely disposing of financial and administrative records when retention is no longer required.

All Employees, Volunteers and Representatives

All employees, volunteers, interns, consultants, contractors, Board members, and other persons acting on behalf of YPDP who have access to personal data shall:

comply with this Policy and applicable data protection requirements;

- a. access personal data only where authorised and necessary for their responsibilities;
- b. Maintain confidentiality of personal data;
- c. Use personal data only for authorised organisational purposes;
- d. Protect passwords, devices, files, and other information resources;
- e. Avoid unauthorised copying, disclosure, transmission, or storage of personal data;
- f. Immediately report actual or suspected data breaches or security incidents;
- g. Participate in relevant data protection and security training; and
- h. Return, delete, or securely dispose of personal data when required.

Failure to comply with these responsibilities may result in appropriate organisational, disciplinary, contractual, or other action.

Third Parties and Data Processors

Third parties, including implementing partners, consultants, contractors, service providers, and other data processors who process personal data on behalf of YPDP shall:

- a. Comply with applicable data protection requirements and contractual obligations;
- b. Process personal data only for authorised purposes and in accordance with agreed instructions;
- c. Maintain appropriate confidentiality and security measures;
- d. Restrict access to authorised personnel;
- e. Notify YPDP promptly of actual or suspected data breaches;

- f. Assist YPDP in responding to legitimate data subject requests and regulatory requirements where applicable;
- g. Not disclose or transfer personal data to another party or jurisdiction except as authorised and permitted by law; and
- h. Securely return, delete, anonymise, or otherwise dispose of personal data when required.

YPDP shall take reasonable steps to assess the data protection practices of third parties before granting them access to personal data and shall monitor compliance where appropriate.

Responsibility for Compliance

Each person and function within YPDP remains responsible for complying with the requirements applicable to their role. Responsibility for data protection shall not be transferred to the Data Protection Officer or Responsible Person merely because that person coordinates the organisation's data protection activities.

Managers shall ensure that personnel under their supervision understand and comply with this Policy, while the designated Data Protection Officer or Responsible Person shall provide guidance, coordination, and oversight.

Where uncertainty exists regarding the collection, use, disclosure, retention, transfer, or security of personal data, personnel shall seek guidance from the designated Data Protection Officer or Responsible Person before proceeding.

19. REPORTING, COMPLAINTS AND ENQUIRIES

Youth Projects Development Platform (YPDP) is committed to ensuring that individuals can raise concerns, ask questions, and exercise their rights in relation to the personal data held or processed by the organisation. YPDP shall provide reasonable and accessible mechanisms through which data subjects and other stakeholders can seek information about the organisation's handling of personal data, raise privacy concerns, or make requests concerning their personal data.

Privacy Enquiries

Individuals may contact YPDP to:

- a. Ask how their personal data is collected, used, stored, shared, retained, or disposed of;
- b. Request information about this privacy and data protection policy;

- c. Seek clarification regarding the processing of their personal data;
- d. Enquire about the organisations or categories of third parties with whom their personal data may be shared; or
- e. Raise any other question relating to privacy and data protection.

YPDP shall provide appropriate information and assistance within a reasonable period and in accordance with applicable legal requirements.

Exercise of Data Subject Rights

A data subject may contact YPDP to exercise any applicable rights recognised under the Data Protection Act No. 3 of 2021 and this Policy, including requests relating to:

- a. Access to personal data held about them;
- b. Correction or updating of inaccurate or incomplete personal data;
- c. Deletion or erasure where applicable;
- d. Withdrawal of consent where processing is based on consent;
- e. Objection to or restriction of processing where applicable; and
- f. Other rights available under applicable data protection law.

Requests should be directed to the person designated by YPDP to manage data protection matters.

Privacy Complaints

Any individual who believes that their personal data has been handled inappropriately, unlawfully, insecurely, or in a manner inconsistent with this Policy may submit a privacy complaint to YPDP.

A complaint may relate to, among other matters:

- a. The unlawful or unnecessary collection of personal data;
- b. Inappropriate use or disclosure of personal data;
- c. Unauthorised access to personal data;
- d. Failure to protect personal data adequately;
- e. Failure to respond appropriately to a data subject request; or
- f. Any other concern regarding YPDP's handling of personal data.

Making a Complaint or Request

Complaints, enquiries, and data subject requests should, where possible, include sufficient information to enable YPDP to understand and investigate the matter. This may include:

- a. The name and contact details of the person making the request or complaint;
- b. A description of the concern or request;
- c. Relevant dates or circumstances;
- d. The specific information or action being requested; and
- e. Any supporting information or documentation available.

YPDP shall not require an individual to provide unnecessary information when making a privacy enquiry or complaint.

Verification of Identity

Where necessary to protect personal data from unauthorised disclosure, YPDP may take reasonable steps to verify the identity of a person making a data subject request before providing access to personal data or taking action on the request. Any information collected solely for identity verification shall be handled securely and shall not be retained longer than necessary for that purpose, subject to applicable legal requirements.

Handling of Complaints and Requests

YPDP shall acknowledge and assess privacy complaints and data subject requests within a reasonable period. The designated Data Protection Officer or Responsible Person shall coordinate the handling of requests and complaints and may consult relevant personnel or functions where necessary. YPDP shall:

- a. assess whether the request or complaint falls within the organisation's responsibilities;
- b. Determine what information or action is required;
- c. Investigate the matter where appropriate;
- d. Maintain confidentiality throughout the process;
- e. Provide a response within the timeframe required by applicable law or, where no specific timeframe applies, within a reasonable period; and
- f. Explain the reasons where a request cannot be fully granted.

No Retaliation

YPDP shall not subject an individual to unfair treatment or retaliation merely because the individual has made a genuine privacy complaint, enquiry, or data subject request. Complaints shall be handled objectively, respectfully, and confidentially, subject to the requirements of applicable law.

Escalation

Where an individual is dissatisfied with YPDP's response or believes that their concern has not been adequately addressed, the individual may be informed of any applicable external complaint or regulatory mechanisms, including the right to approach the Data Protection Commission where appropriate. YPDP shall cooperate with any lawful investigation or complaint process undertaken by the Data Protection Commission or another competent authority.

Record Keeping

YPDP shall maintain appropriate records of significant privacy complaints, enquiries, and data subject requests, including the nature of the matter, actions taken, and outcome where appropriate. Such records shall be protected and retained in accordance with YPDP's data retention requirements.

Contact Point

YPDP shall designate an appropriate contact person or official through whom privacy enquiries, complaints, and data subject requests may be submitted. The organisation shall make the relevant contact details reasonably accessible to data subjects and other stakeholders, including through appropriate organisational communications and, where applicable, the YPDP website.

20. NON-COMPLIANCE AND CONSEQUENCES

Youth Projects Development Platform (YPDP) expects all Board members, management, employees, volunteers, interns, consultants, contractors, partners, and other persons acting on behalf of the organisation to comply with this Privacy and Data Protection Policy and applicable data protection requirements. Failure to comply with this Policy may expose YPDP and affected individuals to legal, financial, operational, reputational, and other risks. YPDP shall therefore take reasonable and proportionate measures to address actual or suspected non-compliance.

Examples of Non-Compliance

Non-compliance may include, but is not limited to:

- a. Accessing personal data without proper authorisation;
- b. Collecting personal data without an appropriate purpose or lawful basis;
- c. Using personal data for an unauthorised purpose;
- d. Disclosing personal data to an unauthorised person or organisation;
- e. Failing to maintain the confidentiality of personal data;
- f. Failing to apply required security measures;
- g. Improperly storing, transferring, retaining, or disposing of personal data;
- h. Failing to report an actual or suspected data breach promptly;
- i. Deliberately or negligently misusing personal data;
- j. Circumventing organisational data protection or security controls; or
- k. Failing to comply with legitimate instructions, procedures, or safeguards established under this Policy.

Investigation of Non-Compliance

Where YPDP becomes aware of suspected material non-compliance, the organisation may conduct an appropriate investigation to establish the circumstances, extent, impact, and cause of the matter. Investigations shall be conducted fairly and confidentially and, where appropriate, may involve management, Human Resources, the designated Data Protection Officer or Responsible Person, ICT, internal or external advisers, or other relevant persons.

Corrective Measures

Depending on the nature and seriousness of the non-compliance, YPDP may take corrective measures including:

- a. Providing guidance, counselling, or additional training;
- b. Requiring remedial action;
- c. Restricting or removing access to personal data or organisational systems;
- d. Strengthening relevant controls or procedures;
- e. Requiring corrective action by a third party or data processor;
- f. Issuing a formal warning or other appropriate management action; or
- g. Referring the matter to the appropriate organisational authority.

Disciplinary and Contractual Consequences

Where non-compliance results from misconduct, negligence, deliberate misuse, or a breach of an individual's employment, volunteer, consultancy, or contractual obligations, YPDP may take disciplinary or contractual action in accordance with applicable organisational policies, contractual terms, and applicable law. Such action may include disciplinary measures, suspension of access or duties, termination of an engagement or contract, or other appropriate action.

Serious or Deliberate Misconduct

YPDP may treat deliberate, reckless, fraudulent, malicious, or seriously negligent misuse or disclosure of personal data as a serious matter. Where appropriate, YPDP may refer such matters to relevant authorities or take legal action, particularly where the conduct may constitute an offence or otherwise give rise to legal liability.

Third-Party Non-Compliance

Where a third party, implementing partner, consultant, contractor, or data processor fails to comply with applicable data protection obligations or contractual requirements, YPDP may require corrective action and may restrict or suspend access to personal data.

Depending on the seriousness of the matter, YPDP may terminate the relevant arrangement or take other contractual or legal measures available to the organisation.

Fair and Proportionate Application

YPDP shall apply consequences for non-compliance in a fair, consistent, and proportionate manner, taking into account:

- a. The nature and seriousness of the violation;
- b. Whether the conduct was intentional, reckless, negligent, or accidental;
- c. The sensitivity and volume of personal data involved;
- d. The actual or potential harm to affected individuals;
- e. Whether the individual or third party reported the incident promptly;
- f. Previous instances of non-compliance; and
- g. Any applicable legal, contractual, employment, or organisational requirements.

The existence of an accidental error or security incident shall not automatically result in disciplinary action where the individual acted in good faith and reported the matter promptly. YPDP shall distinguish between genuine mistakes that require corrective action and deliberate or negligent conduct that warrants disciplinary or other consequences.

Reporting and Escalation

Significant or repeated instances of non-compliance shall be reported to Executive Management and, where appropriate, the Board. Where required by applicable law, YPDP shall also notify or cooperate with the Data Protection Commission or other competent authorities.

21. MONITORING, COMPLIANCE AND POLICY REVIEW

Youth Projects Development Platform (YPDP) shall monitor compliance with this Privacy and Data Protection Policy to ensure that personal data is handled responsibly, securely, and in accordance with applicable legal and organisational requirements. Monitoring shall be proportionate to the nature and scale of YPDP's activities and the risks associated with the processing of personal data.

Monitoring of Compliance

Executive Management, supported by the designated Data Protection Officer or Responsible Person, shall oversee implementation and monitoring of this Policy. Monitoring activities may include:

- a. Reviewing compliance with data protection procedures and controls;
- b. Reviewing how personal data is collected, used, shared, retained, and disposed of;
- c. Monitoring data subject requests, complaints, and privacy concerns;
- d. Reviewing actual or suspected personal data breaches and corrective actions;
- e. Assessing the data protection practices of relevant third parties and processors;
- f. Reviewing access controls and other appropriate security measures;
- g. Identifying emerging data protection risks; and
- h. Assessing whether staff, volunteers, and other relevant persons require additional training or guidance.

Where YPDP establishes an internal audit, compliance, or similar assurance function, that function may support or independently assess compliance with this Policy.

Compliance Reporting

The designated Data Protection Officer or Responsible Person shall provide appropriate reports to Executive Management on significant data protection matters, including:

- a. Material compliance risks;
- b. Significant or repeated breaches of this policy;
- c. Personal data breaches and remedial actions;
- d. Significant complaints or data subject concerns;
- e. Material risks associated with third-party processing or international data transfers; and
- f. Recommendations for strengthening YPDP's data protection arrangements.

Significant data protection matters shall be escalated to the Board where appropriate.

Corrective Action

Where monitoring identifies weaknesses, non-compliance, or areas requiring improvement, YPDP shall take reasonable corrective action. Corrective measures may include updating procedures, improving security controls, providing additional training, restricting access to personal data, strengthening third-party arrangements, or taking other appropriate measures. Where corrective action is assigned to a particular person, department, or third party, implementation shall be monitored to ensure that the identified issue is appropriately addressed.

Policy Review

This Policy shall be reviewed periodically to ensure that it remains relevant, effective, and consistent with YPDP's activities and applicable requirements. The review shall consider:

- a. Changes in applicable laws, regulations, and guidance;
- b. Changes in ydp's organisational structure or activities;
- c. Changes in the types or volume of personal data processed;
- d. Changes in technology and information systems;
- e. Significant data breaches, complaints, or other incidents;
- f. Findings from monitoring, audits, assessments, or reviews;
- g. Changes in relationships with donors, partners, processors, or other third parties; and
- h. Lessons learned from the implementation of the Policy.

Review Triggered by Significant Change

In addition to the scheduled review, YPDP may review this Policy whenever a significant legal, technological, operational, organisational, or data protection development occurs that may affect the adequacy of the Policy. A significant data breach or material change in the way YPDP collects, processes, stores, shares, or transfers personal data may also trigger an earlier review.

Approval of Amendments

Any substantive amendment to this Policy shall be reviewed by Executive Management and the designated Data Protection Officer or Responsible Person, where applicable, and submitted to the Board or other authorised governance body for approval.

Approved amendments shall be communicated to relevant personnel and stakeholders as appropriate.

Version Control and Communication

YPDP shall maintain an appropriate record of approved versions of this Policy, including the date of approval, effective date, review date, and details of substantive amendments. The current approved version shall be made reasonably accessible to relevant personnel and, where appropriate, published on the YPDP website or otherwise communicated to stakeholders.

Continuous Improvement

YPDP shall use findings from monitoring, complaints, data breaches, assessments, audits, training, and operational experience to strengthen its privacy and data protection practices. The organisation shall seek to maintain a culture of continuous improvement, accountability, confidentiality, and responsible management of personal data.