1. INTRODUCTION

1.1. This Data Protection Policy is the overarching policy for data security and protection for Mazao Na Afya Ltd (hereafter referred to as "Mazao").

2. PURPOSE

2.1. The purpose of the Data Protection Policy is to support the Data Security Standards, enshrined in The Data Protection (General) Regulations, 2021, the Data Protection Act, 2019, the common law duty of confidentiality and all other relevant national legislation. We recognize data protection as a fundamental right and embrace the principles of data protection by design and by default.

2.2. This policy covers

2.2.1. Our data protection principles and commitment to common law and legislative compliance;

2.2.2. procedures for data protection by design and by default.

3. SCOPE

3.1. This policy includes in its scope all data which we process either in hardcopy or digital copy, this includes special categories of data.

3.2. This policy applies to all staff, including temporary or otherwise, subsidiaries, strategic partners, our online platforms, third party processors and contractors.

4. PRINCIPLES

4.1. We will be open and transparent with service users and those who lawfully act on their behalf in relation to their care and treatment. We will adhere to our duty of candour responsibilities as outlined in the mission statement.

4.2. We will establish and maintain policies to ensure compliance with the Data Protection Act, 2019, Bill of Rights, Constitution of Kenya, 2010, the common law duty of confidentiality, the General Data Protection Regulation and all other relevant legislation.

4.3. We will establish and maintain policies for the controlled and appropriate sharing of service user, customer, contractor, supplier and staff information with other agencies, taking account all relevant legislation and citizen consent.

4.4. Where consent is required for the processing of personal data we will ensure that informed and explicit consent will be obtained and documented in clear, accessible language and in an appropriate format. The individual can withdraw consent at any time through processes which have been explained to them and which are outlined in our Data Privacy Consent Form: Withdrawal of Consent procedures. We ensure that it is as easy to withdraw as to give consent.

4.5. We will commission annual audits of our compliance with legal requirements.

4.6. We acknowledge our accountability in ensuring that personal data shall be:

4.6.1. Processed lawfully, fairly and in a transparent manner;

4.6.2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

4.6.3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization');

4.6.4. Accurate and kept up to date;

4.6.5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation');

4.6.6. Processed in a manner that ensures appropriate security of the personal data.

4.7. We uphold the personal data rights outlined in the DATA PROTECTION (GENERAL) REGULATIONS, 2021;

4.7.1. The right to be informed;

4.7.2. The right of access;

4.7.3. The right to rectification;

4.7.4. The right to erasure;

4.7.5. The right to restrict processing;

4.7.6. The right to data portability;

4.7.7. The right to object;

4.7.8. Rights in relation to automated decision making and profiling.

Due to our size, we have determined that we are not required to have a Data Protection Officer (DPO), as we do not process special categories of data on a large scale. Nonetheless, to ensure that every individual's data rights are respected and that there are the highest levels of data security and protection in our organization, we have appointed a member of staff to be our Data Security and Protection Lead. The Data Security and Protection Lead will report to the highest management level of the organization. We will support the Data Security and Protection Lead with the necessary resources to carry out their tasks and ensure that they can maintain expertise.

5. UNDERPINNING POLICIES & PROCEDURES

5.1. This policy is underpinned by the following:

5.1.1. Data Quality Policy – outlines procedures to ensure the accuracy of records and the correction of errors;

5.1.2. Record Keeping Policy – details transparency procedures, the management of records from creation to disposal (inclusive of retention and disposal procedures), information handling procedures, procedures for subject access requests, right to erasure, right to restrict processing, right to object, and withdrawal of consent to share;

5.1.3. Data Security Policy – outlines procedures for the ensuring the security of data including the reporting of any data security breach;

5.1.4. Network Security Policy – outlines procedures for securing our network;

5.1.5. Business Continuity Plan –outlines the procedures in the event of a security failure or disaster affecting digital systems or mass loss of hardcopy information necessary to the day to day running of our organization;

5.1.6. Staff Data Security Code of Conduct - provides staff with clear guidance on the disclosure of personal information.

6. DATA PROTECTION BY DESIGN & BY DEFAULT

6.1. We shall implement appropriate organizational and technical measures to uphold the principles outlined above. We will integrate necessary safeguards to any data processing to meet regulatory requirements and to protect individual's data rights. This

implementation will consider the nature, scope, purpose and context of any processing and the risks to the rights and freedoms of individuals caused by the processing.

6.2. We shall uphold the principles of data protection by design and by default from the beginning of any data processing and during the planning and implementation of any new data process.

6.3. Prior to starting any new data processing, we will assess whether we should complete a Data Protection Impact Assessment (DPIA). All new systems used for data processing will have data protection built in from the beginning of the system change.

6.4. All existing data processing has been recorded on our Record of Processing Activities. Each process has been risk assessed and is reviewed annually.

6.5. We ensure that, by default, personal data is only processed when necessary for specific purposes and that individuals are therefore protected against privacy risks.

6.6. In all processing of personal data, we use the least amount of identifiable data necessary to complete the work it is required for and we only keep the information for as long as it is required for the purposes of processing or any other legal requirement to retain it.

6.7. Where possible, we will use pseudonymized data to protect the privacy and confidentiality of our staff and those we support.

7. APPROVAL

7.1. This policy has been approved by the undersigned and will be reviewed at least annually.

Name	
Signature	
Approval Date	
Review Date	