RUIRU-JUJA WATER AND SEWERAGE COMPANY

DATA PROTECTION POLICY

MARCH 2025

Table of Contents

ABBREVIATIONS

AU- African Union

RUJWASCO- Ruiru-Juja Water and Sewerage Company

COK- Constitution of Kenya

DPA- Data Protection Act

DPIA- Data Protection Impact Assessment

DPO- Data Protection Officer

EU – European Union

ODPC- Office of the Data Protection Commissioner

1.0 PREFACE

RUJWASCO recognizes that in this digital age data has become valuable. RUJWASCO generates, collects, stores and transfers data daily. Data generated can range from personal information, financial records, sensitive personal data, and operational data related to water service delivery. As the reliance on data grows, so does the need to protect it from unauthorized access, misuse, and breaches.

The Constitution of Kenya guarantees the right to privacy as a fundamental right. To give effect to this constitutional right under Article 31 (c) and (d), Kenya enacted a comprehensive data protection legislation in 2019 (The Data Protection Act,2019) hereinafter referred to as the ACT which mirrors the EU General Data Protection Regulation (GDPR).

Our commitment to data protection goes beyond compliance with the law. Data breaches can have severe consequences, not only for our staff and stakeholders but also impact our reputation as a trusted water company. Therefore, we have developed a robust data protection policy and stringent security protocols which include continuous staff training to ensure that data is handled responsibly and securely throughout its lifecycle.

Data protection is a collective responsibility that involves the Board of Directors, Senior Management, Staff and other stakeholders. By fostering a culture of data protection and promoting best practices, we can ensure the security and privacy of sensitive information in a rapidly evolving digital world.

Finally, I wish to reaffirm RUJWASCO's commitment to data protection. It is not just a legal requirement but an integral part of our core values as an organization. We will continue to invest in the latest technologies, stringent processes, and a culture of data protection to protect the data entrusted to us.

Chairman,
Ruiru-Juja Water and Sewerage Company

2.0 FOREWORD

In today's digital age, information is more than just data. It represents our personal lives, our business decisions, and our aspirations. As our world becomes increasingly interconnected, the importance of ensuring that this information remains private, secure, and processed with integrity cannot be overstated.

In today's interconnected world, where data plays a pivotal role in shaping businesses and driving innovation, we recognize that trust as one of the foundations to our success.

This Data Protection Policy embodies our commitment to uphold this trust. It is a testament to the steps we take, the technologies we deploy, and the culture we foster to protect the data we are entrusted with. We believe that, by being transparent and proactive in our approach to data protection, we can pave the way for a more secure, responsible, and trusted digital environment.

In the rapidly evolving landscape of digital technology and regulations, we pledge to remain vigilant, agile, and uncompromising in our mission to safeguard personal data.

As we embark on this journey of data protection, every employee is expected to embrace and internalize this policy. We will collectively build a culture that respects privacy and nurtures an environment of trust.
I encourage all stakeholders to familiarize themselves with the details of this Data Protection Policy. Together, we will not only comply with the law but also set new benchmarks in data protection.

Thank you for entrusting RUJWASCO with your data. We take this responsibility seriously and promise to go above and beyond to safeguard your privacy while striving to earn and retain your trust every step of the way.

Simon Mwangi
Managing Director
Ruiru-Juja Water and
Sewerage Company

3.0 PREAMBLE

POLICY BACKGROUND

RUJWASCO is a registered Data Controller and is committed to respecting and protecting the rights of its employees, community, individuals and companies it interacts with in compliance with Article 31 of the Constitution of Kenya, 2010, the Data Protection Act, 2019 and the accompanying statutory regulations and has a further obligation on data processing on:

i. Protecting individual's personal information from unauthorized access or disclosure.
ii. Safeguarding data against breaches, theft, and misuse.
iii. Ensuring that it adheres to legal and regulatory requirements regarding data handling.
iv. Building and maintaining trust with customers, employees, and stakeholders by demonstrating a commitment to protecting their data.
v. Ensuring the accuracy and reliability of data, so it can be trusted for decision-making.

To demonstrate this commitment, RUJWASCO has developed this policy to explain how it collects, uses, and protects personal information. This policy shall be read together with other legal documents including employment contracts, privacy statements for Employees and third-parties, third-party contract agreement and non-disclosure agreements. Where there is a conflict, this policy will prevail.

4.0 POLICY AND LEGAL FRAMEWORK

This policy shall at all times comply with the following:

i. Constitution of Kenya 2010;
ii. Data Protection Act, 2019;
iii. Data Protection (General) Regulations, 2021;
iv. The Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021
v. The Data Protection (Compliance and Enforcement) Regulations, 2021
vi. Access to Information Act, 2019;
vii. Archives Act,1990;
viii. Capital Markets Act as amended; and
ix. other relevant legal instruments.

5.0 POLICY STATEMENT

This policy stipulates the management of Personal Data and the commitment of the Ruiru-Juja Water and Sewerage Company to protect Personal Data of all its data subjects in Kenya and abroad.

6.0 PURPOSE

The purpose of the Data Protection Policy is to provide a framework for the collection and processing of personal data by RUJWASCO and the implementation of the DPA. Towards compliance of the DPA, RUJWASCO should ensure adherence to the highlights of the DPA

namely:

a) Fair and proper use of personal data collected and processed by RUJWASCO.
b) The purpose of data collection should be relevant to its use.
c) Data should be protected against loss and unauthorized access.
d) Subjects should have the right to know what data is collected about him or her.
e) Subjects should have the right to access any data related to him or her.
f) Subjects should be able to challenge the retention of data or amend or erase data about him or her.

7.0 SCOPE

This Policy ensures adequate level of security in terms of confidentiality, availability, and integrity of information assets and personal data of RUJWASCO and those of its employees, community members and third-party stakeholders against data breach.
RUJWASCO establishes, implements, operates, monitors, reviews, maintains, and improves processes and controls related to data processing and information security based on a risk approach.

8.0 DEFINITIONS

"**anonymization**" means the removal of personal identifiers from personal data so that the data subject is no longer identifiable.

"**Biometric data**" means personal data resulting from specific technical processing based on physical, physiological or behavioral characterization including blood typing, fingerprinting, deoxyribonucleic acid analysis, earlobe geometry, retinal scanning and voice recognition;

"**Cabinet Secretary**" means the Cabinet Secretary responsible for matters relating to information, communication, and technology.
"Company" Ruiru-Juja Water and Sewerage Company.

"**consent**" means any manifestation of express, unequivocal, fee, specific and informed indication of the data subject's wishes by a statement or by a clear affirmative action, signifying agreement to the processing of personal data relating to the data subject.

"**data**" means information which –

a) Is processed by means of equipment operating automatically in response to instructions given for that purpose.
b) Is recorded with intention that it should be processed by means of such equipment;
c) Is recorded as part of a relevant filing system;
d) Where it does not fall under paragraphs (a) (b) or (c), forms part of an accessible record; or
e) Is recorded information which is held by a public entity and does not fall within any of paragraphs (a) to (d).

"**Data Commissioner**" means the person appointed under section 6 of the Data Protection Act.

"**Data controller**" means a natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purpose and means of processing personal data.

"**Data processor**" means a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the data controller.

"**Data subject**" means an identified or identifiable natural person who is the subject of personal data.

"**person**" has the meaning assigned to it under Article 260 of the Constitution;

"**Personal Data**" means any information relating to an identified or identifiable natural person.

"Personal Data Breach" means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

"Sensitive Personal Data" means data that reveals the natural person's race, health status, ethnic, social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses' sex, or the sexual orientation of the data subject.

"Processing Data" means any operation or sets of operations performed on personal data whether or not by automated means, such as:

i) collection, recording, organization, structuring;

ii) storage, adaptation, or alteration;

iii) retrieval, consultation, or use;

iv) disclosure by transmission, dissemination, or otherwise making available; or

v) Alignment or combination, restriction, erasure, or destruction

"**Data protection focal point**" means the most senior Company personnel who assists the data controller in carrying out its, his or her responsibilities regarding this Policy.

"**Data protection impact assessment**" means a tool and process for assessing the protection impacts on data subjects in processing their personal data and for identifying remedial actions as necessary to avoid or minimize such impacts.

"**Data Protection Officer**" means a Company personnel who supervises, monitors and reports on compliance with the Data Protection Act and this Policy.

"**encryption**" means the process of converting the content of any readable data using technical means into a coded form.

"**Filing system**" means any structured set of personal data which is readily accessible by reference

to a data subject or according to specific criteria, whether centralized, decentralized, or dispersed on a functional or geographical basis.

“Employee Data”: Personal data collected from employees including but not limited to, contact information, employment history, and performance records.

“**Customer Identification Data**”**:** Personal data collected from customers during water and sewer service applications, including identity card details, KRA PIN, and title deed information.

“Billing Contact Data”: Customer contact details collected for the purpose of sending billing notifications and service updates via SMS.

“**Health data**" means data related to the state of physical or mental health of the data subject and includes records regarding the past, present, or future state of the health, data collected during registration for, or provision of health services, or data which associates the data subject to the provision of specific health services.

"**Identifiable natural person"** means a person who can be identified directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to physical, physiological, genetic, mental, economic, cultural or social or social identity.

“IOSCO” means the International Organization of Securities Commissions.

“**office**" means the office of the Data Protection Commissioner

"**National security organs**" has the meaning assigned to it under Article 239 of the Constitution

“Personal data breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;

“**Processing”** means any operation or sets of operation which is performed on personal data or on sets of personal data whether or not by automated means such as-

a) Collection, recording, organization, structuring;
b) Storage, adaptation or alteration
c) Retrieval, consultation or use;
d) Disclosure by transmission, dissemination, or otherwise making available; or alignment or combination, restriction, erasure or destruction; or
e) Alignment or combination, restriction, erasure or destruction.

“profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person’s race, sex, pregnancy, marital status, health status, ethnic social origin, colour, age, disability, religion, conscience, belief, culture, dress, language or birth; personal preferences, interests, behavior, location or movements;

"**pseudonymization**" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, and such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person;

"**register"** means the register kept and maintained by the Data Commissioner under section 21;

"**restriction of processing**" means the marking of stored personal data with the aim of limiting their processing in the future;

"**Sensitive personal data**" means data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the data subject; and

"**Third Party**" means natural or legal person, public authority, agency or other body, other than the data subject, data controller, data processor or persons who, under the authority of the data controller or data processor, are authorized to process personal data including IOSCO EMMOU signatory members states as the case may be.

9.0 PRINCIPLES OF DATA PROTECTION

There are seven (7) Principles of data protection in Kenya. The seven (7) principles are drawn from the **EU General Data Protection Regulation (GDPR), 2016.** The principles are:

a) **Lawful and Fair Processing**; this refers to the ethical and legal principles that organizations must adhere to when collecting, processing, handling, and disclosing personal information of individuals. All processing of personal data should be lawful and fair. It should be transparent to individuals that personal data concerning them are collected or otherwise processed and to what extent the personal data is or will be processed.
b) **Purpose Specification**: Personal data needs to be collected for specified, explicit and legitimate purposes and should not be processed in a way incompatible with those purposes.
c) **Data minimization**: Data collected shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
d) **Accuracy:** Personal data should be recorded as accurately as possible and where necessary, updated to ensure it fulfils the purpose(s) for which it is collected.
e) **Storage and Limitation-** Data relating to a data subject must be deleted, archived or anonymized once it has served its purpose.
f) **Integrity and Confidentiality-** Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage and using appropriate technical or organizational measures.
g) **Accountability-** the data controller is responsible for and must demonstrate compliance with

the principles of Data Protection.

10.0 DATA PROTECTION OFFICER

RUJWASCO, being a data controller and data processor, shall appoint or designate a data protection officer (hereinafter referred to as DPO). The DPO shall; -

a) Advise RUJWASCO, employees and stakeholders, on the data processing requirements provided under this Act or any other written law.
b) Inform and advise RUJWASCO and the employees who carry out processing of their obligations pursuant to this Act.
c) Ensure on behalf of RUJWASCO that this Act is complied with.
d) Facilitate capacity building of employees involved in data processing operations.
e) Provide advice on the Data Protection Impact Assessments (DPIAS), monitor its performance if required, and co-operate with the Commissioner with regard to the performance of the DPIA.
f) Co-operate with the Data Commissioner and any other authority on matters relating to the protection of personal data.
g) Be the contact point for the data subjects and the Data Protection Commissioner.
h) Ensure RUJWASCO responds to requests from data subjects exercising their rights under the Act.
i) Be involved in the monitoring and evaluation of the systems that process and manage personal data at RUJWASCO.
j) And any other function as required by the Act.

11.0 DUTY TO NOTIFY

RUJWASCO, before collecting personal data shall inform the data subject of:

a) The rights of the data subject specified under section 26 of the Data Protection Act.

b) The fact that RUJWASCO is collecting personal data and the purpose for which the personal data is being collected.

c) The third party whose personal data has been or will be transferred to, including details of safeguards adopted where applicable.

d) The contacts of the data controller or data processor and on whether any other entity may receive the collected personal data.

e) A description of the technical and organizational security measures taken to ensure the integrity and confidentiality of personal data.

f) The data being collected pursuant to any law and whether such collection is voluntary or mandatory.

g) The consequences, if any, where the data subject fails to provide all or any part of the requested data.

h) This information shall be provided through privacy notices, consent forms, or other appropriate means, ensuring transparency and accessibility

i) A notification by RUJWASCO to the Data Commissioner of a data breach.

12.0 COLLECTION OF INFORMATION

RUJWASCO shall collect personal information with knowledge of the subject when they do any of the following:

1. Application for recruitment, either directly from candidates or sometimes from an employment agency or background check provider, additional information may be collected from third parties, including former employers, credit reference agencies and other background credit agencies.
2. Job-related activities throughout the period of working with RUJWASCO.
3. Employee benefits offered by RUJWASCO.
4. Fill the Bio-Data sheet.
5. Enroll on the Biometric system.
6. Provide notifications of; Birth, death, sick-sheets and any other documents required as evidence for effective leave administration.
7. Access the Company premises through the gate.
8. Book for reservation, use or visit of Company facilities/services.
9. Receive Support by RUJWASCO through community-based projects.
10. Attend community meetings convened by RUJWASCO and its partners;
11. Sponsored by RUJWASCO through educational initiatives.
12. Open an account with RUJWASCO for the purpose of water and sanitation Services
13. Respond to procurement and disposal processes published by RUJWASCO
14. Contracts with RUJWASCO for the Supply of goods and services

13.0 USE OF INFORMATION

RUJWASCO collects and processes data for the following reasons:

1. Facilitate recruitment and fulfillment of the employment contract;
2. Maintain accurate and up-to-date employment records and contact details (including details of whom to contact in the event of an emergency (including spouse and or next of kin information), and records of employee contractual and statutory rights;
3. Operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace;
4. Operate and keep a record of employee performance and related processes to plan for career development, succession planning, and workforce management purposes;
5. Ensure that we comply with legal requirements in relation to individuals with disabilities and to meet our legal obligations under Occupational Safety and Health Law;
6. Operate and keep a record of other types of leave (including maternity, paternity, adoption, study, and compassionate leave) to allow effective workforce management and to ensure that we comply with duties concerning leave/off duty entitlement;
7. Ensure effective general human resources and business administration;
8. Provide references on request for prospective, current or former employees;
9. Respond to and defend against legal claims;
10. Maintain and promote equality in the workplace;
11. Capture attendance for benefit administration.
12. Capture names, banking details, credit limits and any other personal information needed for business purposes for suppliers, clients and other third-party stakeholders.
13. Provision of water and Sanitation Services
14. Generate reports for purposes of reporting to donors;
15. Carry out community surveys relevant to the Company's objectives;
16. GPS placement of Company meters and other appurtenances
17. Household composition for demographic
18. Bank details for the purpose of deposit refunds

14.0 SENSITIVE DATA

RUJWASCO keeps sensitive data such as:

1. Medical information (Pre and Periodic Medical check reports), for purposes of Occupational Safety and Health Act, 2007.
2. Injuries sustained at work (for reporting to the directorate of safety and health),
3. Disability information (for tax benefit and audit purposes as per the provisions of the Persons with Disabilities Act, 2003),
4. Sick off details, routine medical check reports.
5. Employee Bio-data forms.
6. Spouse's contact and that of your next of Kin for purposes of benefit administration and service continuity where need arises.

7. Biometric details for capturing attendance and for payroll administration.
8. Name, age, physical address and sex for purposes of contract administration.
9. Name, bank details and credit limits of clients
10. We may routinely publish some sources of information about the Company that include personal data. These may consist of audio-visual representations of our events, prospectuses, impact reports, newsletters and staff profiles on our website/ social media sites.

15.0 CATEGORIES OF DATA COLLECTED

1. Personal details collected:
   - Name, title, physical address, contact details including email address, telephone number, date of birth, gender, disability status and age.
2. Academic and professional qualifications, skills, experience and employment history, including start and end dates with previous employers.
3. Remuneration, including entitlement to benefits such as medical, pension and/or insurance cover.
4. Identity card or passport number
5. KRA Pin number
6. Bank account details
7. Company ownership Details (CR12)
8. Social Health Insurance number
9. Next of kin, dependents and emergency contacts
10. National Social Security Fund Number
11. Periods of leave taken, including sickness absence, off duty, annual leave, etc.
12. Details of disciplinary or grievance procedures, any warnings issued and related correspondences.
13. Assessments of performance, i.e. - appraisals, performance reviews and ratings, performance improvement plans.
14. Medical or health information and conditions.
15. Data collected in accident reports and risk assessments.
16. Gps location of meters installed on Customer premises
17. Number of individuals in a household

16.0 LAWFUL AND FAIR PROCESSING OF PERSONAL DATA

When processing personal data, RUJWASCO will ensure that:

a) There is an appropriate legal basis or legitimate interests clearly connected to the specific purpose of the processing of personal data such as consent, contract, legal obligation or in the exercise of authority.

b) The data subject is granted the highest degree of autonomy possible with respect to control over their personal data.

c) The data subject knows what they consented to and there is an easy means to withdraw consent.

d) restricting processing where the legal basis or legitimate interests ceases to apply.

e) The processing of personal data is done in a fair manner and does not adversely affect the rights and freedoms of the data subject.

f) RUJWASCO shall not process personal data unless the data subject consents to processing for one or more specified purposes.

17.0 MINIMIZATION OF COLLECTION

At the point of data collection, RUJWASCO will ensure the following elements are implemented.

a) RUJWASCO will limit the amount of personal data collected to what is necessary for the purpose.

b) RUJWASCO shall demonstrate the relevance of the data to the processing in question.

c) The personal data shall be Pseudonymized as soon as it is no longer necessary to have directly identifiable personal data removed.

d) Anonymizing or deleting personal data where the data is no longer necessary for the purpose.

e) Making data flows efficient to avoid the creation of more copies or entry points for data collection than is necessary, and the application of available and suitable technologies for data avoidance and minimization.

18.0 ACCURACY OF DATA

RUJWASCO shall ensure that the data collected is accurate. The elements necessary to implement the principle of data accuracy shall include the following but not limited to:

a) Ensuring data sources are reliable including verifying Employee Data with employees, Health Data with medical providers, Customer Identification Data with government records, and Billing Contact Data with customers.

b) Recording personal data accurately;

c) Verification of the correctness of personal data with the data subject before and at different stages of the processing depending on the nature of the personal data, in relation

to how often it may change.

d) Erasing or rectifying inaccurate data without delay.

e) Mitigating the effect of an accumulated error in the processing chain.

f) Giving data subjects an overview and easy access to personal data in order to control accuracy and rectify as needed.

g) The use of technological and organizational design features to decrease inaccuracy.

19.0 SAFEGUARD AND SECURITY OF PERSONAL DATA

The Company shall safeguard personal data to ensure privacy, protect the right of the data subjects and maintain trust. This shall include but not limited to the following:

a) **Access Controls**: Only authorized individuals shall have access to personal data. This will be managed with authentication and authorization.
b) **Firewalls and Intrusion Detection Systems**: to prevent unauthorized external access to networks and systems.
c) **Physical Security** such as locking servers in a secure room, especially for very sensitive data.
d) **Data Breach Response Plan**: Including identifying and closing the security hole, notifying affected users, and potentially notifying the relevant authorities.
e) **Anonymization and Pseudonymization**: Involving replacing identifiers in the dataset so that the individuals to whom the data belong can't be directly identified.
Pseudonymization is a method where personally identifiable information fields within a data record are replaced by one or more artificial identifiers, or pseudonyms.
Anonymization is the process of removing personally identifiable information from data sets, so that the individuals whom the data describe remain anonymous.
f) **Data Minimization**: Only collect the minimum amount of personal data needed for specific purposes.
g) **Employees Training**: Ensuring that all employees are trained in data protection and understand the importance of their role in maintaining privacy.
h) **Regular Audits and Updates**: Regular checks on systems and processes to ensure they are functioning as intended. Keeping systems and software updated is also critical to ensure that vulnerabilities are patched.
i) **Encryption**: This is a technique to convert data into a code to prevent unauthorized access. Data in transit and at rest shall be encrypted to protect them from interception or breaches.

20.0 CONSENT

a) The Company shall obtain express consent from the Data Subject prior to processing personal data and sensitive personal data

b) The processing of personal data shall be for the specific purposes for which consent was given.

c) Where a new purpose is required, the Company shall first notify and obtain subsequent express consent of the data subject.

d) In taking a data subject through the consent form the following shall be explained to the data subject:

i. **Purpose of Data Collection**. -The Company shall clearly state the purpose for which data is being collected, ensuring it is specific, explicit, and legitimate.

ii. **Voluntary Consent-**Data subjects' consent will be given freely without any coercion, and they will have the option to withdraw consent at any time without any adverse consequences. Where lack of consent will prevent the Company from providing services to the data subject, this shall be stated.

iii. **Informed Consent**-The Company shall provide clear and easily understandable information about the data processing activities, including the types of data collected, the purposes, the data recipients and the data retention periods.

iv. **Opt-In Mechanism-** Consent will be obtained through appropriate means including a signature, ticking of boxes or using of the words "YES" or "NO".

v. **Age Verification-** If the data processing involves individuals under the age of consent, the Company shall obtain parental or guardian consent.

vi. **Separate Consents** -Separate consents will be obtained for different processing activities, ensuring that data subjects can give granular consent for each purpose.

vii. **Right to Withdraw Consent-**Data subjects will be informed of their right to withdraw consent at any time and the process to do so will be clearly explained.

viii. **Revoking Consent-**The Company shall notify data subjects of the possibility to revoke their consent, and the withdrawal will be acknowledged and acted upon promptly.

ix. **Conditional Services-**The Company will not condition the provision of services or benefits on the data subject's consent to processing that is unnecessary for the performance of the service.

x. **Notification of Changes-** In case of any changes to the data processing that may affect the original consent, data subjects will be notified and asked for renewed consent if necessary.

xi. **Recordkeeping-**The Company shall maintain records of all obtained consents, including the time, date, and method of obtaining consent.

xii. **Data Subject's Rights -**Data subjects shall be informed of their data protection rights, including the right to access, rectify, erase, restrict processing, and data portability.

xiii. **Language and Presentation -**The consent provisions will be presented in clear and straightforward language, avoiding legalese or technical jargon.

xiv. **Data Protection Officer (DPO)-**Data subjects will be provided with the contact details of the Data Protection Officer (DPO) to address any concerns or inquiries regarding their data.

a) There shall be a regular audit and verification on the accuracy and completeness of consent records.
b) There shall be a periodic review and update of consent practices to align with changes in data processing activities or regulations.
c) The policy acknowledges that there will be exceptional circumstances where personal data can be processed without the data subjects' consent. There may be limitations on data subject rights when required by the law or when there are competing rights and therefore it will require an assessment based on the facts and circumstances. Any exceptions to the requirement for consent shall be clearly documented and justified in accordance with the Data Protection Act, 2019.

21.0 DATA PROTECTION IMPACT ASSESSMENT (DPIA)

DPIA is a systematic process used to identify and assess the potential risks and impacts of a data processing activity on individuals' privacy and data protection rights. Where a processing operation is likely to result in high risk to the rights and freedoms of a data subject, by virtue of its nature, scope, context, and purposes the Company shall, prior to the processing, carry out a data protection impact assessment. The Data Protection Impact Assessment shall be carried out in accordance with the Data Protection Act and the regulations and guidelines issued thereunder.

22.0 REPORTING CONCERNS AND NON-COMPLIANCE

Below is the procedure for reporting any data concerns or non-compliance:

a) Every employee has a responsibility to promptly report any data protection concerns or instances of non-compliance that come to their attention. This includes issues related to data handling, security breaches, unauthorized access, or any other data protection-related matter.
b) All employees are encouraged to report any concerns related to data protection or instances of non-compliance with the data protection policy immediately upon noticing the non-compliance to their immediate supervisor in writing.
c) The supervisor shall report all concerns or non-compliance reports to the Data Protection Officer immediately upon detection or notification but not later than twenty-four hours of notification or detection.
d) All reports made will be treated with confidentiality and protection. Whistleblowers will be shielded from retaliation, and their identities will be kept confidential.
e) The Company shall provide an option for anonymous reporting to encourage employees who

may be hesitant to report concerns openly and the Company shall have a clear whistleblower protection policy to ensure that individuals who report concerns are protected from retaliation.

f) All reports, investigations, and actions taken to address concerns and non-compliance will be documented and maintained in a secure and confidential manner.

g) Employees who report concerns will receive feedback on the status and outcome of the investigation, to the extent allowed by applicable laws and regulations.

23.0 PROCESSING AND TRANSFERRING PERSONAL DATA OUT OF KENYA

The Company, in executing its mandate, may transfer personal data to external third parties in other countries. Before transfer, the Company shall:

a) Give sufficient proof to the Data Commissioner on the appropriate safeguards with respect to the security and protection of personal data;

b) Ensure that the required degree of protection is afforded to personal data under the laws of that country. The third-party service providers to whom a data transfer is made should have appropriate safeguards in place to protect personal data;

c) Ensure that the processing of sensitive personal data out of Kenya shall only be effected upon obtaining consent of the concerned data subject;

d) Before conducting international data transfers, the Company may conduct a data transfer impact assessment to evaluate the risks associated with the transfer and implement necessary measures to ensure data protection; and

e) The processing of sensitive personal data out of Kenya shall be effected upon approval by the Data Commissioner.

24.0 DATA BREACH MANAGEMENT

Below is the procedure for handling data breach;

a) Employees are required to notify the DPO as soon as possible upon becoming aware of a data breach and to properly record the breach.

b) The Company shall without undue delay and, where feasible, not later than 72 (seventy- two) hours after having become aware of it, notify the Office of the Data Commissioner of the breach of personal data.

c) The Company in its capacity as a data processor shall notify the data controller within 48 Hours of the breach.

d) The notification referred above shall at least:

    i. describe the nature of the personal data breach.

ii. description of the measures taken by the data controller to address the data breach.

iii. recommendation on the measures to be taken by the data subject to mitigate the adverse effects of the security compromise.

iv. where applicable the identity of the unauthorized person who may have accessed or acquired the personal data; and

v. the name and contact of the data protection officer.

e) If a personal data breach is likely to result in personal injury or harm to a data subject, the Company shall within a reasonable time notify the data subject in writing of the data breach and take mitigating measures as appropriate without undue delay. In such cases, the data controller should also notify the Data Protection Officer of the personal data breach**.**

f) The data controller shall maintain a data breach register recording the facts relating to the breach, its effects and the remedial action taken.

25.0 TRAINING AND AWARENESS

The Company shall conduct a training session to senior management and employees to equip them with the necessary skills to handle personal data responsibly. On onboarding, new employees shall be sensitized on data protection requirements depending on their role. Awareness campaigns shall be conducted to promote a culture of data protection within the Company.

26.0 DATA PARTNERS

The Company may engage data partners to process data on its behalf or on execution of its mandate. The Company shall ensure that the required degree of protection is afforded to personal data. The Company will ensure that third party service providers to whom a data transfer is made has appropriate safeguards in place to protect personal data. Data Processing Agreements with data partners shall include specific provisions regarding data security, confidentiality, and compliance with the Data Protection Act, 2019.

27.0 ROLES AND RESPONSIBILITIES

The implementation framework outlines the hierarchy and responsible departments, committees, sections, units and individuals facilitating and overseeing the implementing this Policy is as follows:

27.1 Board of Directors

The role of the Board will be:

i. To approve the Policy once presented by management.

27.2 Managing Director

The role of the Managing Director will be to:

i. Appoint a Data Protection Officer.

ii. Appoint the Data Protection Committee.
iii. Approve resources for Data Protection activities
iv. Oversee compliance with the provisions of the Data Protection Act, 2019

27.3 Role of the Data Protection Officer

The role of the Data Protection Officer will be as outlined under clause 10 of this policy.

27.4 Role of the Data Protection Committee

The Committee shall:

i. Participate in the development and review of the Company's Data Protection Policy.
ii. Ensure sensitization of the Board and employees and relevant stakeholders of the Company.
iii. Support the implementation of and reinforce commitment to the Data Protection Policy.
iv. Monitor and advise relevant parties on changes on the legal framework on data protection in Kenya; and
v. Monitor and evaluate the implementation of this policy.

27.5 Heads of Departments and Divisions/ Units

They will be required to ensure compliance with Data Protection Act, 2019 and General Regulations 2021 in their day-to-day operations.

27.6 Employees

They will be required to:

i. Fully comply with the provisions of the Data Protection Act, 2019 and General Regulations 2021.
ii. Participate in capacity building and sensitization sessions when called upon;
iii. Report any data protection breach as provided for.

28.0 DATA RETENTION

The Company will be committed to ensuring compliance with data retention in line with the provisions of the Data Protection Act and any other related legislation. In particular**;**

a) Personal data that is not recorded in individual case files is not to be retained longer than necessary for the purposes for which it is collected.
b) All individual case files, whether open or closed, are considered permanent records and must be retained in accordance with the Public Archives Act.
c) Where specific legislation guides on data retention the provisions shall apply

29.0 MONITORING AND COMPLIANCE

The Data Protection Officer will continuously monitor the implementation of this policy. The Data Protection Committee will assist the Data Protection Officer to conduct periodic evaluation with a view to assessing the relevance, efficiency, effectiveness, impact and sustainability of the provisions of this policy.

30.0 POLICY REVIEW

This policy will be reviewed every three (3) years or when need arises.

Policy Approval and Effective Date

This Policy comes into effect on this …… day of..... **2025.**

MANAGING DIRECTOR **BOARD CHAIRMAN**

31.0 APPENDICES

I. DATA PROTECTION TEMPLATES FOR DATA SUBJECTS

A. PHOTOGRAPHY & VIDEO RELEASE FORM

I hereby grant permission to the rights of my image, likeness and sound of my voice as recorded on audio or video tape without payment or any other consideration. I understand that my image may be edited, copied, exhibited, published or distributed and waive the right to inspect or approve the finished product wherein my likeness appears. Additionally, I waive any right to royalties or other compensation arising from or related to the use of my image or recording. I also understand that this material may be used in diverse marketing, promotional and educational settings within an unrestricted geographical area.
Photographic, audio or video recordings may be used for the following purposes:

a. Social media channels including but not limited to Facebook, Instagram, X, YouTube, WhatsApp, TickTock etc.

b. RUJWASCO website and or partner affiliated sites

c. PowerPoint presentations

d. Marketing materials (posters, adverts etc.) including videos

e. Annual reports, community newsletters, staff newsletters

f. Media publications and features

g. All uses will relate to RUJWASCO and its affiliated brands.

By signing this release, I understand that this permission signifies that photographic and video recording of me may be electronically displayed via the Internet and or printed materials.
I will be consulted about the use of photographs and video recordings for any other purpose other than those listed above.
There is no time limit on the validity of this release nor is there any geographic limitation on where these materials may be distributed.
This release applies to photographic, audio and video recording collected as part of the sessions listed on this document only.
By signing this form, I acknowledge that I have read and completely understood the above release and agree to be bound thereby. I hereby release any and all claims against any person or organization utilizing this material for education purposes.

Name _____
Street Address/P.O. Box /Physical Address _____
City: _____
Postal address_____
Phone: _____
Email Address:

Signature: _____
Date: _____

If this release is obtained from a presenter under the age of 18 years, then the signature of that presenter. Parent and or legal guardian is required.
Parent/Guardian signature: _____
Date: _____
Policy Approved by Managing Director: ……
Date: …….

B. REQUEST FOR RESTRICTION OR OBJECTION TO THE PROCESSING OF PERSONAL DATA

Note

(i) Documentary evidence in support of the objection may be required.

(ii) Where the space provided for in this Form is inadequate, submit information as an Annexure

A. NATURE OF REQUEST

Mark the appropriate box with an "x". Request for:

RESTRICTION ☐ OBJECTION ☐

B. DETAILS OF THE DATA SUBJECT

Name: .....

Identity Number: .....

Phone number: .....

E-mail address: .....

(Your details below where initiating the request for a minor or a person who has no capacity)

Name:.....

Relationship with the Data Subject

Contact Information:

C. REASONS FOR THE REQUEST

(Please provide detailed reasons for the restriction or objection)

D. DECLARATION

I certify that the information given in this application is true

Signature……..

Date…….

C. REQUEST FOR ACCESS TO PERSONAL DATA

Note:

(i) Documentary evidence in support of this request may be required.

(ii) Where the space provided for in this Form is inadequate, submit information as an annexure

(iii) All fields marked as * are mandatory

A. DETAILS OF THE DATA SUBJECT

(This section is to provide the details of the Data Subject).

Name*: …….

ID*: ……

Phone number*: ……

E-mail address: …….

(Provide the following details where making a request on behalf of a minor or a person who has no capacity)

Name*; ……

Relationship with the Data Subject*; …….

Contact Information*; ……

B. DETAILS OF THE PERSONAL DATA REQUESTED

(Describe the personal data requested)

MODE OF ACCESS

I would like to: (check all that apply)

[ ] Inspect the record

[ ] Listen to the record

[ ] Have a copy of the record made available to me in the following format:

[ ] Photocopy(Please note copying costs will apply) No. of copies required: .....

[ ] Electronic

[ ] Transcript (Please note that transcription charges may apply)

[ ] Other (specify) .....

C. Delivery Method

[ ] Collection in person

[ ] By mail (provide address where different / in addition to details provided above)

Town/City: .....

[ ] By e-mail (provide email address where different / in addition to details provided above):

.....

DECLARATION

Note any attempt to access personal data through misrepresentation may result in prosecution.

I certify that the information given in this application is true.

Signature…….

Date ……

D. REQUEST FOR RECTIFICATION

(i) Documentary evidence in support of this request may be required.

(ii) Where the space provided for in this form is inadequate, submit information as an annexure

(iii) All fields marked as * are mandatory

A**. DETAILS OF THE DATA SUBJECT**

Name*: ……

Identity Number*:……

Phone number*:……

E-mail address:……

(Provide the following details where making a request on behalf of a minor or a person who has no capacity)

Name* ……

Relationship with the Data Subject*……

Contact Information*……

Signature*…….

Date*……

PROPOSED CHANGE (S)

	Personal data to be corrected e.g. name, residential status, and mobile number, email address.	Proposed change	Reason for the proposed change
1.			
2.			
3.			
4.			
5.			

B. DECLARATION

Note any attempt to rectify personal data through misrepresentation may result in prosecution.

I confirm that I have read and understood the terms of this request form and certify that the information given in this application is true.

Signature:…….

Date ……..

E. REQUEST FOR DATA PORTABILITY

a. Documentary evidence in support of this request may be required.
b. Where the space provided for in this Form is inadequate, submit information as an Annexure
c. All fields marked as * are mandatory

A. DETAILS OF THE DATA SUBJECT

(This section is to provide the details of the Data Subject).
Name*: ……
Identity Number*:……
Phone number*:……
E-mail address:……..
(Provide the following details where making a request on behalf of a minor or a person who has no capacity)
Name* ……
Relationship with the Data Subject*……
Contact Information* ……..

B. DETAILS OF THE REQUEST

Please transfer a copy of my personal data to …….
By either:
• Emailing a copy to them at ……
• Mailing to: ……
• Others (Please specify) …….

DECLARATION

Note, any attempt to port personal data through misrepresentation may result in prosecution.
I certify that the information given in this application is accurate to the best of my knowledge.
Signature…….
Date……

F. REQUEST FOR ERASURE OF PERSONAL DATA

(i) Documentary evidence in support of this request may be required.
(ii) Where the space provided for in this Form is inadequate, submit information as an annexure
(iii) All fields marked as * are mandatory

i. **DETAILS OF THE DATA SUBJECT**

(This section is to provide the details of the Data Subject).
Name*: .....
Identity Number*: .....
Phone number*: .....
e-mail address: .....
(Provide the following details where making a request on behalf of a minor or a person who has no capacity)
Name* .....
Relationship with the Data Subject* .....
Contact Information* .....

ii. REASON FOR ERASURE REQUEST

(Tick the appropriate box)
(a) Your personal data is no longer necessary for the purpose for which it was originally collected [ ].
(b) You have withdrawn consent that was the lawful basis for retaining the personal data [ ].
(c) You object to the processing of your personal data and there is no overriding legitimate interest to continue the processing; [ ].
(d) The processing of your personal data has been unlawful [ ].
(e) Required to comply with a legal obligation. [ ].

PERSONAL DATA TO BE ERASED

Describe the personal data you wish to have erased.

DECLARATION

Note any attempt to erase personal data through misrepresentation may result in prosecution.
I confirm that I have read and understood the terms of this request form and certify that the information given in this application is true.
Signature…… Date……

II. DECLARATION OF CONFIDENTIALITY

I hereby acknowledge that my engagement as an Employee [ ]: Service Provider [ ]: Stake Holder [ ]: Business partner [ ], of RUJWASCO, I may be entrusted with confidential information pertaining to the Company or other significant matters during a specified period. Such confidential information may include but is not limited to:

1. Business and Professional secrets of RUJWASCO and its partners, clients, employees, community and suppliers.

2. Financial data.
3. Personnel data including Employee Personal Data.
4. Payroll data.
5. Any other sensitive information about the Company.

I hereby undertake to:

I. Respect confidentiality of all information obtained in the course of my engagement with RUJWASCO:

II. Not under any circumstances divulge any of this information or discuss it with any unauthorized individual:

III. Not to leave the information where it is visible or otherwise easily accessible to unauthorized individuals;

IV. Not use the information for purposes that are not associated with my work duties or engagement with RUJWASCO.

I further acknowledge that I fully understand all of the above and that a breach of this undertaking will result in disciplinary and or Legal action being taken against me by the Company.

Name: _____

Department: _____

Signature: _____