



Greenpark Water Services Limited

P.O Box 1916 – 20117, Naivasha.

Tel: +254718467606

Email: manager@greenparknaivasha.com

GREEN PARK DATA PROTECTION POLICY – (GPWS DPP – 2025 V1)

1. Purpose

This Data Protection Policy outlines the commitment of Green Park Water Services Limited to ensure the lawful, fair, and secure handling of personal data in the provision of **security, road maintenance, and water supply services** to **shareholders and residents**. It is intended to safeguard the privacy rights of all individuals whose data we handle, in compliance with the **Data Protection Act, 2019 (Kenya)** and other applicable laws.

2. Scope

This policy applies to:

- All **shareholders, residents, employees, contractors, and service providers**.
- All **personal data** processed by the company, whether in physical or electronic form.
- All company departments, especially those involved in security, operations, customer service, billing, and administration.

3. Definitions

- **Personal Data:** Any information related to an identifiable individual (e.g., name, phone number, meter number, house number).
- **Data Subject:** An individual whose personal data is collected (e.g., shareholder, resident, employee).
- **Data Controller:** Green Park Water Services Limited, determining how and why personal data is processed.
- **Processing:** Any action performed on personal data, including collection, use, storage, sharing, or deletion.
- **Data Processor:** A third party that processes personal data on behalf of the company (e.g., billing software vendors, security system providers).



4. Legal Basis for Data Collection and Use

Personal data will only be processed on one or more of the following legal bases:

- Fulfillment of the service agreement or shareholder obligations.
- Legal obligations (e.g., tax, security compliance, health and safety).
- Legitimate interest (e.g., community safety, billing accuracy). □ Consent (for optional communications or non-core services).

5. Categories of Data Collected

Depending on the nature of engagement, we may collect the following:

- **Shareholders and Residents:** Full name, contact info, house/plot number, ID number, water consumption, service requests, CCTV footage or similar.
- **Employees and Contractors:** ID, phone number, background check data, work logs, payment information or similar.
- **Visitors and Guests:** Entry/exit logs, vehicle registration, CCTV images or similar.

6. Data Protection Principles

All personal data will be:

- Processed lawfully, fairly, and transparently.
- Collected for specific, clear purposes and not further used for unrelated activities.
- Adequate, relevant, and limited to what is necessary.
- Accurate and regularly updated.
- Kept only for the required period.
- Children's personal data shall require parental or guardian consent - Additional safeguards shall be implemented to protect children's data, including limited data collection, access restrictions, and enhanced security protocols Stored and handled securely.

7. Shareholder Data Confidentiality

The company is committed to maintaining the **confidentiality of shareholder information**:

- Personal details and account records will not be disclosed without proper authorization.
- Voting records, financial contributions, and meeting attendance are stored securely and accessible only to authorized individuals.



8. Security Measures

We implement the following to secure data:

- Password protection, restricted system access, and role-based permissions.
Encrypted backups and secure storage for physical files.
- CCTV footage stored securely and accessed only by authorized personnel.
Staff training on data protection and privacy awareness.
- Sensitive personal data, including biometric, health, and financial information, shall be processed with enhanced safeguards such as encryption, restricted access, and regular audits, in accordance with Section 45 of the DPA.

9. Data Sharing

Personal data may only be shared with:

- Approved contractors or third parties under strict confidentiality agreements.
- Government agencies where required by law.
- Legal processes
- Shareholder-authorized bodies (e.g., audit or committees), with proper documentation.

All third-party data processors engaged by the Company shall be bound by written contracts requiring compliance with the Data Protection Act, including obligations on data security, confidentiality, and breach notifications. The Company shall monitor processor compliance periodically.

10. Rights of Data Subjects

All shareholders, residents, employees, and other data subjects have the right to:

- Request access to their data.
- Correct or update their data.
- Request deletion where legally allowed.
- Object to certain types of processing.
- Withdraw consent (if consent was the legal basis).
- Lodge a complaint with the Office of the Data Protection Commissioner.

11. Data Breach Notification

Any suspected or actual data breach shall be:

- Reported immediately to the Data Protection Officer (DPO).
- Investigated and documented.



- Communicated to affected persons and authorities where necessary, as per legal timelines.

12. Data Retention

Personal data will be retained only as long as necessary to fulfill service, legal, or operational needs.

Data Type	Retention Period
CCTV	30 Days
Billing Records	7 Years
Employee Records	Term of Employment + 7 Years
Shareholder Data	Term of Shareholding + 7 Years

Redundant or outdated records will be securely destroyed or deleted.

13. Consent Management

The Shareholders shall provide to the Company consent in the format attached in Annex A. A parental or guardian consent form is appended as Annex B. Consent shall be explicit, informed, and freely given. All consent forms shall be clearly documented and stored physically and/or electronically

14. Appointment of Data Protection Officer (DPO)

Captain (Rtd) Chris Gathecha is appointed as the **DPO**, responsible for ensuring compliance with this policy and addressing any data-related queries or complaints.

Contact: manager@greenparknaivasha.com

15. Compliance and Enforcement

The Company shall establish clear internal reporting channels for data breaches and policy violations. Disciplinary actions, including potential legal consequences, shall follow documented escalation procedures to ensure accountability and enforcement of this policy.

16. Review and Updates

This policy is referred to as DPA version “2025-v1” and shall be reviewed annually or upon changes in relevant legislation or company operations.



