

Privacy Policy

neighbourguard.co.za

How NeighbourGuard collects, uses, and protects your personal information under POPIA.

COMPLIANCE · 01 OF 06

Version 1.0 — May 2026

Draft for legal review. This document is a template prepared by NeighbourGuard for review and adaptation by an admitted attorney before publication. The text reflects POPIA, Act 4 of 2013 and its Regulations as at May 2026. Do not rely on this draft until a qualified legal practitioner has signed it off.

NeighbourGuard is a South African community-safety platform. We process personal information so that members can summon help, so that responders can reach the people who need them, and so that tenant administrators can run their communities. This Policy explains what we collect, why, who we share it with, how long we keep it, and the rights you have under **the Protection of Personal Information Act, 4 of 2013 ("POPIA")**.

CONTENTS

- | | |
|------------------------------------|---------------------------------|
| 1. Who we are | 10. Direct marketing |
| 2. Scope of this Policy | 11. Your rights |
| 3. Personal information we process | 12. Complaints to the Regulator |
| 4. Lawful basis for processing | 13. Security |
| 5. Purposes | 14. Breach notification |
| 6. Recipients | 15. Cookies and analytics |
| 7. Cross-border transfers | 16. Changes to this Policy |
| 8. Retention | 17. Contact |
| 9. Children's data | |

1 — WHO WE ARE

Responsible Party (Operator)	Dales Programming and Robotics Club House (Pty) Ltd, trading as NeighbourGuard
CIPC registration	2023/536470/07
SARS income tax	9385152229
B-BBEE certificate	9436600581 · Level 1 Contributor
Registered office	01 Madeliefie Street, Riamar Park, Bronkhorstspuit, 1020, Gauteng, South Africa
Website	https://neighbourguard.co.za
Information Officer	Simon Lesedi Babedi · CEO · sl.babedi@neighbourguard.co.za
Deputy Information Officer	[to be appointed before launch]

The Information Officer is registered (or in the process of registration) with the Information Regulator of South Africa as required by section 55 of POPIA.

2 — SCOPE OF THIS POLICY

This Policy applies to all personal information that NeighbourGuard processes when you:

- create or use a NeighbourGuard account (member, activator, responder, tenant administrator);
- use any NeighbourGuard channel — web portal, mobile application, USSD (*120*... shortcode), WhatsApp bot, SMS notifications, voice alerts, push notifications;
- interact with us through email, telephone, web forms, social media, or in person;
- visit a NeighbourGuard-operated site (training session, demonstration, hardware install).

For neighbourhood-watch tenants ("Tenant") who run their own community on the platform, NeighbourGuard acts as an **Operator** (processor) for the Tenant's member data and as a **Responsible Party** (controller) for account, billing, audit, and platform-operations data.

3 — PERSONAL INFORMATION WE PROCESS

We process the categories listed below. Items marked † are **special personal information** under section 26 of POPIA and require additional safeguards.

CATEGORY	EXAMPLES	SOURCE
Identity	Full name, ID number †, date of birth	Data subject
Contact	Mobile, email, physical address, residential complex/unit	Data subject or Tenant admin
Location	GPS of registered premises, activation event coordinates	Device · USSD/Cell-ID · manual entry
Account	Username, password hash, role, permissions, login history	Platform-generated
Activation	Date/time, menu position (arm/disarm/trigger/panic), zone, originating channel, response actions	Platform-generated
Responder	Name, contact number, channel preferences, response history	Tenant admin / responder
Vehicle / property	Registration number, descriptions of premises	Tenant admin / member
Imagery †	Profile photos, incident photos (where uploaded)	Direct upload
Children's data †	Minor household occupants registered by a member	Parent / guardian
Technical	IP address, device identifier, browser, app version, push token	Device
Communications	WhatsApp/SMS message bodies, voice-alert metadata, support tickets	Data subject
Payment	Banking details for subscription / donation collection (FNB)	Tenant admin

We do **not** process biometrics, criminal history, religious belief, race, sexual orientation, trade-union membership, or health information, except where a member voluntarily supplies it in a medical-emergency context.

4 — LAWFUL BASIS FOR PROCESSING (SECTION 11 POPIA)

We rely on the following grounds, applied per processing activity:

- **Consent** — opt-in to WhatsApp messaging, marketing communications, optional analytics.
- **Contractual necessity** — operating your account and delivering the safety service you signed up for.
- **Legitimate interest** — community safety, fraud prevention, security of the platform, defending legal claims.
- **Legal obligation** — tax records, lawful interception requests, court orders.
- **Protection of a legitimate interest of the data subject** — emergency response routing where consent cannot first be obtained (a panic activation, for example).

For each processing activity we maintain a record of the legal ground in our **Processing Register** (see 02 — *Data Protection Procedures*).

5 — PURPOSES

1. Route emergency activations to the correct zone responders and, where authorised, to emergency services.
2. Operate the USSD, WhatsApp, SMS, voice, and push-notification channels.
3. Generate reports for tenant administrators (zone activity, response times, false-activation rates).
4. Authenticate users, including 2FA, password reset, and session security.
5. Bill subscriptions, process donations, and account for VAT.
6. Comply with court orders, SAPS requests under the Cybercrimes Act, and lawful regulatory enquiries.
7. Improve and secure the platform, detect abuse, audit access.
8. Send service announcements and, with consent, marketing about new features.

6 — RECIPIENTS OF PERSONAL INFORMATION

We disclose personal information only to the categories below, under written processing agreements where the recipient acts as an Operator:

RECIPIENT	ROLE	LOCATION
Tenant administrators (your neighbourhood-watch committee)	Joint Responsible Party / Operator	South Africa
Zone responders assigned by your tenant	Recipient (event data only)	South Africa
Meta Platforms Ireland Ltd (WhatsApp Business API)	Operator	EU / USA
Telnyx Communications LLC (SMS / voice)	Operator	USA / EU
Hosting provider [to be confirmed at launch]	Operator	South Africa / EU
Absolute Hosting (SmarterMail email)	Operator	South Africa
Payment gateway [to be confirmed at launch]	Operator	South Africa
SAPS / Metro Police / Emergency services	Recipient (event-driven)	South Africa
Auditors, attorneys, accountants under confidentiality	Recipient	South Africa
Information Regulator, courts, lawful authorities	Recipient (where required)	South Africa

We do **not** sell personal information.

7 — CROSS-BORDER TRANSFERS (SECTION 72 POPIA)

WhatsApp messaging routes through Meta servers in the EU and USA. Telnyx routes SMS and voice via international PoPs. We rely on the section 72 grounds:

- the recipient is subject to a law, binding corporate rules, or binding agreement that provides an adequate level of protection substantially similar to POPIA (Meta's Data Processing Addendum; Telnyx DPA);
- the transfer is necessary for performance of the contract with you (i.e. delivering a WhatsApp alert you requested);
- you have consented to the transfer where consent is the applicable ground.

A copy of each Operator agreement is available to data subjects on written request.

8 — RETENTION

DATA CLASS	RETENTION	TRIGGER TO DELETE
Account profile	Duration of account + 5 years	Last login + 5 yr or erasure request
Activation events	7 years	Closing of any related incident or dispute
Audit logs (security)	12 months minimum, 5 years where reasonably required	Time-based
WhatsApp / SMS message bodies	90 days in hot store, 12 months archived	Time-based
Voice recordings (where enabled)	90 days	Time-based
Billing / tax records	5 years (Tax Administration Act)	Statutory
CCTV (offices, where applicable)	30 days	Time-based
Support tickets	3 years	Closure + 3 yr
Marketing-consent records	Life of consent + 3 years	Withdrawal + 3 yr

Where you exercise your right to erasure, we will delete or de-identify within the timelines in section 11, except where we are legally required to retain (for example, tax records).

9 — CHILDREN'S DATA (SECTION 34 POPIA)

We do not knowingly process personal information of children (under 18) without prior written consent of a competent person (parent or legal guardian). Where a member registers a minor household occupant, the registering member warrants that they are a competent person. A parent or guardian may withdraw consent and require deletion at any time by emailing the Information Officer.

10 — DIRECT MARKETING (SECTION 69 POPIA)

We will only send direct marketing by electronic means with your prior opt-in consent or where you are an existing customer and we are marketing similar products to you with a clear opt-out in each message. Opt out at any time by:

- replying **STOP** to any SMS;
- replying **STOP** to any WhatsApp message;
- clicking "unsubscribe" in an email;
- emailing the Information Officer.

11 — YOUR RIGHTS AS A DATA SUBJECT

Under POPIA you have the right to:

- be notified that we process your information (this Policy);
- access the personal information we hold about you (Form 2 of the POPIA Regulations);
- request correction or deletion of inaccurate, outdated, excessive, misleading, or unlawfully obtained information;
- object to processing on reasonable grounds (Form 1);
- object to direct marketing (Form 4);
- not be subject to a decision based solely on automated processing that has legal consequences;

- complain to the Information Regulator (Form 5);
- institute civil proceedings.

To exercise any right, email the Information Officer. We will respond within **30 calendar days**. For complex requests we may extend by a further 30 days and will notify you in writing. A reasonable fee may apply to access requests in line with the prescribed tariff.

12 — INFORMATION REGULATOR COMPLAINT CHANNEL

Information Regulator	Information Regulator of South Africa
Physical	JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001
Postal	PO Box 31533, Braamfontein, 2017
General enquiries	enquiries@inforegulator.org.za
Complaints	complaints.IR@inforegulator.org.za
Web	https://inforegulator.org.za

13 — SECURITY

The technical and organisational measures protecting your information are listed in *06 — Data Security Protocols*. In summary: TLS 1.2+ in transit, encryption at rest, role-based access control, 2FA for administrators, audit logging of every privileged action, and breach notification per section 22 POPIA.

14 — BREACH NOTIFICATION

If we have reasonable grounds to believe that personal information has been accessed or acquired by an unauthorised person, we will notify the Information Regulator and affected data subjects as soon as reasonably possible after discovery (typically within 72 hours of confirmation), unless a public body responsible for prevention, detection or investigation of offences directs otherwise.

15 — COOKIES AND ANALYTICS

The web portal uses strictly necessary cookies for authentication and session management. Optional analytics cookies, where enabled, require your consent via the cookie banner. We do not use advertising cookies.

16 — CHANGES TO THIS POLICY

We will publish material changes on the website and notify active users at least 14 days before they take effect.

17 — CONTACT

Information Officer

Name: Simon Lesedi Babedi (CEO)

Email (corporate): sl.babedi@neighbourguard.co.za

Email (primary): lesedi.simon@gmail.com

Phone: +27 63 594 1451

Postal & web

Registered office: 01 Madeliefie Street, Riamar Park, Bronkhorstspuit, 1020, Gauteng

Web: neighbourguard.co.za

Privacy email alias: privacy@neighbourguard.co.za (to be provisioned)

NeighbourGuard is a trading name of **Dales Programming and Robotics Club House (Pty) Ltd**, CIPC reg 2023/536470/07. This Privacy Policy is governed by the laws of the Republic of South Africa, in particular the Protection of Personal Information Act, 4 of 2013 ("POPIA") and its Regulations. This document is a draft template prepared for legal review and is not effective until approved by an admitted attorney and published with a formal effective date.