Acceptable Use Policy

neighbourguard.co.za

What you may and may not do with the NeighbourGuard platform, and what we'll do if you cross the line.

COMPLIANCE · 08 OF 14
Version 1.0 — May 2026

Draft for legal review. Specific suspension thresholds in §6 and §9 reflect our current operating capacity; an attorney should pressure-test them against CPA s51 and POPIA s9.

False alarms are not a joke. Every NeighbourGuard activation fans out to dozens of phones and, depending on tier configuration, an armed-response operator. Deliberately firing a false alarm wastes responder time, dilutes trust in the platform, and may constitute the offence of giving false information to a peace officer under SAPS Act regulations. We treat it as a material breach — see §6.

Plain-language summary (CPA s22). Use the platform for what it's built for — coordinating community safety. Do not fire fake alarms. Do not use the broadcast features to send spam, hate speech, or political content. Do not share your account credentials. If you do any of these, we will warn you, then suspend you, then close your account.

This Acceptable Use Policy ("AUP") sets the conduct rules for every person interacting with the NeighbourGuard platform — tenant administrators, business members, household members, and responders. It supplements *04 — Terms of Service* and is incorporated into it by reference. Breach of this AUP is breach of the Terms and gives us the rights described in §6 below.

1 — SCOPE

This AUP applies to every feature of the platform, including but not limited to: the web portal, the mobile application, the USSD shortcode, the WhatsApp Business number, SMS short-codes, the broadcast hub, voice fan-out via Telnyx, the public marketing site, and any tool offered through the platform. It binds you whether you access the platform as an individual, on behalf of a tenant, or as a responder volunteering your time.

2 — ACCEPTABLE USES

The platform exists to coordinate community-safety incidents. You may use it to:

- Fire an alarm activation when you genuinely believe a person, household, or asset is at risk.
- Receive, acknowledge, or escalate alerts as a responder.
- Administer a tenant — invite members, configure zones, manage responder layers, run audit reviews.
- Broadcast safety-relevant notices to your zone (incident summaries, patrol reminders, drill schedules).
- Configure household speed-dial, USSD codes, and personal preferences.
- Use the Schedule-a-Demo or lead-magnet tools to evaluate the platform before signing up.

3 — PROHIBITED CONDUCT

You may not, and you must not permit any other person to:

3.1 Misuse of activations

- Fire an activation when no genuine threat exists — including for drills not formally announced as drills, for pranks, or to test responder attentiveness without prior agreement from your tenant administrator.

- Fire activations outside the geographic zone in which you are registered, where the platform offers cross-zone targeting and you are not authorised to use it.
- Cause an activation by automated means (bot, script, scheduler) — only a human pressing a button or dialling a code may activate.

3.2 Misuse of broadcast features

- Send messages that are unrelated to community safety — including commercial advertising, political campaigning, religious solicitation, or fundraising.
- Send messages that contain hate speech, incitement to violence, harassment of a named person, or material covered by section 16(2) of the Constitution.
- Send messages that defame an individual or an organisation.
- Send bulk messages of any kind without WhatsApp Business opt-in, where the platform's WhatsApp channel is in use — see *03 — WhatsApp Business API Compliance*.

3.3 Security and integrity

- Share, sell, or transfer your account credentials. Each person uses their own account; the platform is not licensed for shared use.
- Probe, scan, or test the vulnerability of the platform without prior written consent from the Information Officer. Coordinated disclosure is welcomed — see *06 — Data Security Protocols* §10.
- Attempt to bypass authentication, access an account that is not yours, or read data that is not yours to read.
- Introduce malware, run a denial-of-service attack, or fuzz the platform's public endpoints.
- Scrape or systematically extract data from the platform (member directories, responder lists, zone maps) for any purpose.

3.4 Identity and impersonation

- Impersonate another person, including by registering with someone else's phone number, ID number, or email address.
- Provide false or misleading information during registration — false name, false ID number, false next-of-kin, false household location.
- Hold yourself out as a tenant administrator if you are not appointed, or as a responder if you are not on a responder roster.

3.5 Unlawful content and conduct

- Use the platform to commit, plan, or facilitate any offence under South African law.
- Upload, link to, or transmit child sexual abuse material, terrorist content, or other unlawful imagery.
- Process personal information of any third party through the platform in a way that breaches POPIA — for example, by uploading a contact list you do not have the right to upload.

4 — TENANT-ADMINISTRATOR OBLIGATIONS

Tenant administrators carry additional responsibilities because they configure the platform for many members:

- You must keep your member roster current — remove members who leave, suspend members who breach this AUP within their tenant.
- You must maintain a responder roster that reflects who has actually accepted the responder role. Do not list a contact who has not agreed.
- You must use the broadcast hub only for safety-relevant notices to your tenant. If you wish to send commercial or political content, use a separate channel — your tenant agreement does not licence the platform for that.
- You must respond to data-subject requests routed to you within the timeframes in *01 — Privacy Policy* §10.
- You must report a suspected breach to the Information Officer within 24 hours of becoming aware.

5 — RESPONDER OBLIGATIONS

If you accept a responder role:

- You must respond in good faith, to the best of your ability, within the response window agreed for your responder layer.

- You may not use information learnt during a response (a member's address, household composition, vulnerable persons present) for any purpose other than the response itself.
- You may not record audio or video of a response without the consent of the member receiving the response, save where you are required by law or by the response (e.g., body-cam wear for an armed-response operator).
- You may resign from the responder role at any time by notifying your tenant administrator. Resignation does not relieve you of confidentiality obligations.

6 — ENFORCEMENT

If we believe in good faith that you have breached this AUP, we may take any one or more of the following steps, in any order, without prior notice if the breach is serious:

STEP	WHEN WE USE IT	WHAT HAPPENS
Warning	First-time minor breach	An email and in-app notice naming the breach and the clause. You have 7 days to remedy.
Feature restriction	Repeated minor breach, or first material breach	We disable the specific feature you misused (broadcast, fire-alarm, USSD) while keeping the rest of your account live. Restriction lasts 14 days or until you confirm in writing that the breach will not recur.
Suspension	Material breach, or third repeated breach	Account locked. You can read but cannot transact. Suspension lasts up to 30 days while we investigate.
Termination	Confirmed serious breach (§3.1 false alarm, §3.3 security, §3.5 unlawful)	Account closed. We honour any refund due under *10 — Refund & Cancellation Policy* §3. We may report to SAPS if conduct is criminal.

Severity is judged on the harm caused (number of people affected, whether emergency services were dispatched, whether personal information was breached), the recency of any prior breach, and the user's role (administrators and responders are held to a higher standard than ordinary members).

7 — APPEALS

If we take an enforcement step against you, you may appeal in writing within 14 calendar days to **support@neighbourguard.co.za**. The appeal is heard by a person who was not involved in the original decision. We will respond within 14 calendar days with a final outcome. The appeal does not pause the enforcement step unless we expressly say so.

8 — REPORTING OTHER USERS

If you believe another user is breaching this AUP, report it to **support@neighbourguard.co.za** with: the user's tenant and account identifier (or the alarm event ID), what they did, and when. We treat reports confidentially and investigate every credible one. False or vexatious reports are themselves a breach — §3.4 above.

9 — AUTOMATED ABUSE-DETECTION

We run automated rate-limits, honeypots, and bot-detection on every public endpoint. Triggering these systems repeatedly may result in temporary IP-level or account-level blocks. Blocks are lifted automatically once normal behaviour resumes; if you are blocked in error, contact support and we will lift the block within one business day.

10 — UPDATES

We update this AUP whenever the platform's feature set changes materially. Updates are versioned in the header. Where an update narrows what is permitted, we will give 14 calendar days' notice on the site and by email to tenant administrators. Where an update only clarifies an existing rule, it takes effect immediately on publication.

Report abuse

Email: support@neighbourguard.co.za

Phone: +27 63 594 1451

Hours: 08h00–17h00 weekdays

NeighbourGuard

Office: 01 Madeliefie Street, Riamar Park, Bronkhorstspruit, 1020, Gauteng

Web: neighbourguard.co.za

NeighbourGuard is a trading name of **Dales Programming and Robotics Club House (Pty) Ltd**, CIPC reg 2023/536470/07. This policy is incorporated into and forms part of *04 — Terms of Service* and is governed by the laws of the Republic of South Africa.