Nimbl Mail - Acceptable Use Policy

Effective Date: 20 May 2026 **Last Updated:** 20 May 2026 **Company:** Nimbl (Pty) Ltd **Service:** Nimbl Mail - Email Marketing Platform **Website:** nimbl.one

---

1. Overview

Nimbl Mail is a permission-based email marketing platform. We provide tools for businesses to send legitimate marketing emails, newsletters, and transactional messages to recipients who have given their explicit consent to receive such communications.

This Acceptable Use Policy (AUP) applies to all users of the Nimbl Mail platform and governs the use of our email sending infrastructure.

2. Permitted Use

Nimbl Mail may only be used to send:

- Marketing emails and newsletters to recipients who have opted in (explicit consent)
- Transactional emails related to an existing business relationship (order confirmations, account notifications, etc.)
- Informational emails to recipients who have a reasonable expectation of receiving communication from the sender

3. Prohibited Use

The following activities are strictly prohibited:

- **Unsolicited bulk email (spam):** Sending emails to recipients who have not given prior consent
- **Purchased or scraped lists:** Using email lists that were purchased, rented, harvested, or scraped from websites
- **Misleading content:** Emails with deceptive subject lines, forged headers, or misrepresented sender identity
- **Illegal content:** Any content that violates South African law, including the Protection of Personal Information Act (POPIA), the Electronic Communications and Transactions Act (ECTA), or the Consumer Protection Act (CPA)
- **Malware distribution:** Emails containing viruses, malware, phishing links, or other malicious content
- **Harassment:** Threatening, abusive, or harassing communications
- **Adult content:** Unsolicited adult or sexually explicit material
- **Fraud:** Emails promoting fraudulent schemes, pyramid schemes, or deceptive practices

4. Consent Requirements

All senders on Nimbl Mail must:

- Only send to recipients who have given verifiable opt-in consent
- Maintain records of consent (date, source, method) for all recipients
- Honour unsubscribe requests within 2 business days (our platform processes these immediately)
- Include a visible, functional unsubscribe link in every marketing email
- Include the sender's valid physical address or registered business address

5. Technical Standards

All emails sent through Nimbl Mail:

- Are authenticated with SPF, DKIM, and DMARC
- Include proper List-Unsubscribe headers
- Are rate-limited per sender to prevent abuse
- Are subject to bounce and complaint monitoring

6. Compliance with South African Law

POPIA (Protection of Personal Information Act)

- All subscriber data is processed in accordance with POPIA
- Data subjects can request access to, correction of, or deletion of their personal information
- An Information Officer is designated for each account
- Data is stored on South African or EU-based infrastructure

ECTA (Electronic Communications and Transactions Act)

- All commercial emails comply with Section 45 of ECTA
- Opt-out mechanisms are provided as required by law

7. Monitoring and Enforcement

Nimbl Mail actively monitors sending activity for:

- High bounce rates (>5% triggers review, >10% triggers suspension)
- Spam complaint rates (>0.1% triggers review, >0.3% triggers suspension)
- Blacklist appearances
- Content quality and compliance

8. Abuse Handling (see Section 9)

We take abuse seriously. Any reported or detected violation of this AUP will result in:

1. **First offence:** Warning and required remediation within 24 hours
2. **Second offence:** Temporary suspension of sending privileges
3. **Severe or repeated offence:** Permanent account termination

9. Abuse Reporting and Handling Mechanism

How to Report Abuse

Anyone can report abuse from our platform:

- **Email:** abuse@nimbl.one
- **Website:** nimbl.one/abuse

Handling Process

1. **Acknowledgement:** All abuse reports are acknowledged within 4 business hours
2. **Investigation:** Our compliance team investigates the reported content and sender within 24 hours
3. **Action:** Depending on severity:
    - Sending is suspended immediately for the account in question
    - The sender is notified and required to provide evidence of consent
    - If no valid consent exists, the account is terminated
4. **Resolution:** The reporter is notified of the outcome within 48 hours
5. **Escalation:** Unresolved complaints can be escalated to our Information Officer

Automated Protection

- **Feedback loops:** We process ISP feedback loops (FBLs) and automatically suppress complainants
- **Bounce management:** Hard bounces are automatically suppressed after first occurrence
- **Blacklist monitoring:** We monitor major blacklists and take immediate action on any listing
- **Rate limiting:** Per-account send limits prevent any single user from impacting deliverability for others

Contact

Abuse Reports: abuse@nimbl.one **General Enquiries:** support@nimbl.one **Information Officer:** privacy@nimbl.one

---

Nimbl (Pty) Ltd reserves the right to update this policy at any time. Users will be notified of material changes.