

ACCEPTABLE USE POLICY

Last updated 12 September 2026

Policy reference: POL-TECH-02

Applies to: all visitors, customers, clients, candidates, vendors and authorised users of RVZ platforms

Terms reference: clause 12

Governing law: ECTA 25 of 2002; Cybercrimes Act 19 of 2020; POPIA

This Acceptable Use Policy sets the fair and secure rules for using rvzgroup.co.za, shop.rvzgroup.co.za, the client, vendor, candidate and staff portals, our application programming interfaces, email and messaging channels, and any other system provided or connected by RVZ International Group (Pty) Ltd ("RVZ") (together, the "Platforms"). It forms part of our Terms and Conditions (clause 12) and binds every visitor and user. Authorised team members and contractors are additionally bound by the internal edition of POL-TECH-02 and the staff systems rules in section 8.

1. Permitted use

You may access and use the Platforms for lawful personal or business purposes: browsing, enquiring, ordering, booking, applying for a vacancy, managing your account and communicating with us (Terms clause 12.1). Limited personal use by staff is permitted where it is lawful, reasonable and does not impair security, cost or performance.

2. Prohibited conduct

You must not, and must not attempt to or help anyone else to:

- Break the law. Use the Platforms for any purpose that is unlawful in South Africa or in the place from which you access them, or in breach of these rules.
- Compromise security. Access or attempt to access any account, system, data or area you are not authorised to access; probe, scan or test the vulnerability of a system without authorisation (section 6); bypass or interfere with authentication, access controls, rate limits, payment controls or CSRF protection; or intercept data. These acts are offences under Cybercrimes Act 19 of 2020 sections 2 to 7 and ECTA sections 86 to 88.
- Introduce malicious code or software — viruses, worms, ransomware, trojans, spyware, logic bombs or any tool designed to disrupt, damage or gain unauthorised access (Cybercrimes Act section 4).
- Disrupt service. Launch or facilitate a denial-of-service attack, flood forms or endpoints, place fraudulent or bulk test orders, or otherwise impose an unreasonable load (Cybercrimes Act section 5; ECTA section 86(5)).
- Commit fraud or impersonate. Use a stolen or unauthorised payment method; open an account in another person's name; misrepresent your identity, authority or affiliation; forge headers or message origins; or impersonate RVZ, its staff, a division or another user (Cybercrimes Act sections 8 and 9; common-law fraud).
- Misuse personal information. Collect, harvest, scrape or store personal information of other users, staff or candidates, or process it in breach of POPIA, including for direct marketing without a lawful basis (POPIA section 69).

- Send spam or unlawful communications. Use our forms, email or messaging to send unsolicited commercial communications, chain messages or bulk messages in breach of ECTA section 45, POPIA section 69 or CPA section 11.
- Post or transmit harmful content. Content that is defamatory; that incites violence, damage to property or hatred on a prohibited ground; that constitutes harassment, threats or intimate images shared without consent (Cybercrimes Act sections 14 to 16; Protection from Harassment Act 17 of 2011); that is obscene, child sexual abuse material or otherwise prohibited under the Films and Publications Act 65 of 1996; or that is discriminatory in breach of PEPUDA.
- Infringe rights. Upload, share or reproduce content that infringes copyright, trade marks, designs, patents, trade secrets, privacy or personality rights; or use RVZ's content, marks or brand assets outside what our Copyright Notice permits.
- Reverse engineer, decompile, disassemble or create derivative works of the Platforms' software except to the limited extent section 19B of the Copyright Act permits for interoperability.
- Resell or frame. Resell access, frame or mirror the Platforms, or remove proprietary notices, without our written consent.
- Interfere with others. Obstruct any other user's use, or harass, abuse or threaten RVZ staff, suppliers or other users.

3. Accounts, credentials and security

3.1 You are responsible for everything done through your account. Keep your credentials confidential; do not share an account; use a strong, unique password and, where offered, two-factor authentication; and log out on shared devices (Terms clause 12.2).

3.2 Notify us promptly at support@rvzgroup.co.za if you suspect your credentials or account have been compromised. We may require reasonable verification through a separate trusted channel before changing sensitive account, banking or payment details, and we will never ask you for your full password.

3.3 You must provide accurate registration information and keep it current. Accounts may be opened only by a person aged 18 or over, or by a minor with the assistance of a parent or guardian as the law requires (Terms clause 3). One person may not maintain multiple accounts to evade a restriction.

3.4 Business accounts (client, vendor) must be operated only by persons the business has authorised; the business is bound by the acts of a user it has permitted to use its credentials.

4. Content you submit

4.1 You retain ownership of content you upload (briefs, artwork, logos, CVs, reviews, messages) and grant RVZ the limited licence in Terms clause 15.2 to use it to provide the service. You warrant that you hold the rights and any consents needed and that the content is accurate and lawful (Terms clause 15.3).

4.2 Reviews, testimonials and public comments must be genuine, reflect your own experience and not be paid for or fabricated. Under CPA section 41 and the ARB Code, fake or misleading endorsements are unlawful; we remove them.

4.3 Uploaded files are scanned and restricted by type and size; we may remove or refuse content that breaches this policy, that we are legally required to remove, or that poses a security risk, and we may preserve it as evidence.

5. Automated access, scraping and AI training

5.1 Automated access is permitted only through an API we publish, in accordance with its documentation and rate limits, or by well-behaved search-engine crawlers that respect robots.txt. Scraping at harmful scale, circumventing rate limits, or extracting a substantial part of any database or product catalogue is prohibited (Terms clause 12.1).

5.2 Except as expressly permitted in robots.txt or llms.txt, the Platforms' content, images and data may not be collected to train, fine-tune or evaluate machine-learning or AI models, or to build a competing dataset or

service. Personal information on the Platforms may never be collected for these purposes.

5.3 Price-comparison and aggregation services may not present RVZ products or prices in a way that is inaccurate or misleading, or that suggests an affiliation.

6. Security research and responsible disclosure

6.1 We welcome good-faith reports of security vulnerabilities. If you believe you have found one, email support@rvzgroup.co.za with "Security" in the subject line, describing the issue and how to reproduce it. We will acknowledge within 3 business days, keep you informed, and credit you if you wish once the issue is fixed.

6.2 Good-faith research means: stop as soon as you have confirmed the issue; do not access, modify, download or delete data beyond what is strictly necessary to demonstrate it; do not degrade service; do not use social engineering, phishing or physical intrusion; do not exploit the issue or disclose it publicly before we have had a reasonable opportunity (normally 90 days) to fix it; and do not demand payment. Research conducted within these limits is authorised for the purposes of Cybercrimes Act section 2 and ECTA section 86, and we will not pursue legal action against you for it. Testing outside these limits is not authorised.

7. Monitoring, investigation and privacy

7.1 We log access to the Platforms (IP address, user agent, pages and actions, timestamps), scan uploads and monitor for security, fraud, abuse and performance. We may investigate suspected breaches of this policy lawfully and proportionately, and preserve and use logs as evidence. Monitoring is disclosed here in accordance with POPIA section 18 and the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 ("RICA"); see our Communications and Recording Notice and Privacy Policy.

7.2 We cooperate with law-enforcement and regulators as the law requires, including under Cybercrimes Act Chapter 5 (preservation and disclosure orders), RICA and the Criminal Procedure Act 51 of 1977, and we may report suspected offences.

8. Authorised users of RVZ systems (staff, contractors, placed workers)

In addition to the rules above, an authorised user of RVZ-provided or RVZ-connected technology must: use it primarily for authorised work; never share credentials, bypass controls, install unapproved software, connect unauthorised devices or disable protection; never create, access, store or transmit unlawful, discriminatory, harassing, sexually exploitative, malicious or infringing material; send confidential and personal information only to authorised recipients through approved secure methods; verify unusual payment, credential or data requests through a separate trusted channel before acting (business-email-compromise control); and report suspected compromise, misdelivery or loss immediately. RVZ may monitor and investigate its systems lawfully and proportionately for legitimate purposes with appropriate notice; users retain their legal rights to privacy. A breach is handled under the disciplinary code or contract; good-faith reporting of mistakes is never penalised. Use of AI tools is governed by our Responsible AI Policy.

9. Enforcement

9.1 If you breach this policy we may, proportionately to the breach: issue a warning; remove or edit content; rate-limit, suspend or terminate your account or access; cancel pending orders or bookings where fraud or abuse is reasonably suspected; block IP addresses or devices; recover our reasonable costs of investigation and remediation from you; report the matter to payment providers, platforms, regulators or law enforcement; and pursue civil or criminal remedies (Terms clause 21).

9.2 Where a consumer's access is suspended or terminated we give notice and reasons unless doing so would prejudice an investigation or the law prohibits it, and we do not withhold a refund, deliverable or record to which the consumer is legally entitled.

9.3 You indemnify RVZ against claims and losses arising from your breach of this policy to the extent Terms clause 20 provides and the law permits.

10. Availability, links and take-down notices

10.1 We aim for reasonable availability but may conduct maintenance or respond to incidents; no uninterrupted-availability warranty is given except under a paid service level or mandatory law (Terms clause 12.3).

10.2 Third-party services linked or embedded in the Platforms remain subject to their own terms; a link is not an endorsement (Terms clause 12.4).

10.3 Take-down. If you believe content on the Platforms infringes your rights, send a notice identifying the work, its location on the Platforms, the basis of your ownership, your contact details and the action requested, in the form contemplated by ECTA section 77 (Terms clause 12.6). We may preserve evidence, restrict access and request verification before acting. A person who knowingly submits a materially false take-down notice is liable for resulting damages under ECTA section 77(2), and RVZ does not make retaliatory or misleading take-downs.

11. Reporting abuse

Report abuse, spam, phishing that imitates RVZ, security concerns or policy breaches to support@rvzgroup.co.za. Phishing and impersonation of RVZ may also be reported to the South African Police Service and, for websites, to the domain registrar or ZADNA. Victims of online harassment may apply for a protection order under the Protection from Harassment Act 17 of 2011.

12. Legal references

- Electronic Communications and Transactions Act 25 of 2002 — ss 43–46 (consumer protection online), 45 (unsolicited communications), 70–79 (limitation of liability of service providers and take-down notification) and 85–89 (cyber inspectors and cyber crime, including unauthorised access, interference and denial of service).
- Cybercrimes Act 19 of 2020 — ss 2–7 (unlawful access, interception, interference with data and systems, unlawful acquisition and use of passwords and access codes), 8–9 (cyber fraud, forgery and uttering), 11–12 (aggravated offences and attempts), 14–16 (malicious communications) and Chapters 4–5 (jurisdiction, preservation and disclosure).
- Protection of Personal Information Act 4 of 2013 — ss 9–25, 69 and 71–72; Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 — ss 4–6 (consent and business-purpose interception).
- Consumer Protection Act 68 of 2008 — ss 11 (right to restrict unwanted direct marketing), 41 (false, misleading or deceptive representations) and 48–51 (fair terms and prohibited transactions).
- Copyright Act 98 of 1978 (including s 19B computer-program exceptions); Trade Marks Act 194 of 1993 ; Films and Publications Act 65 of 1996 as amended; Protection from Harassment Act 17 of 2011 ; Promotion of Equality and Prevention of Unfair Discrimination Act 4 of 2000 s 10 (hate speech) and s 11 (harassment).
- Master Terms and Conditions — clauses 3 (eligibility), 12 (website, accounts and electronic communications), 15 (intellectual property), 20 (indemnities) and 21 (suspension and termination).

This policy is the public edition of RVZ's Acceptable Use of Technology and Communications policy (POL-TECH-02) and forms part of our Terms and Conditions. It reflects the law as at the date shown above and is not legal advice.

Generated 24 September 2026 at 12:47 by RVZ International Group (Pty) Ltd

This document is published at <https://rvzgroup.co.za/legal/acceptable-use.php>, which remains the authoritative version. It is provided for information and is not a substitute for independent legal advice.