

JOJO CONNECT Acceptable Use Policy

Version: 2.0

Effective date: September 2026

Last updated: September 2026

This Acceptable Use Policy applies to every person using JOJO CONNECT, whether through a captive portal, account, package, voucher, integrated router, support channel or related service.

1. Lawful and responsible use

Use JOJO CONNECT only for lawful purposes and in a way that does not harm people, equipment, networks, services or data. You are responsible for activity performed through your device, account, voucher or authorised session.

2. Prohibited activity

You must not use, or attempt to use, the service for fraud; identity theft; phishing; malware; unauthorised access; credential collection; deliberate service disruption; denial-of-service activity; unauthorised scanning; interception of traffic; bypassing captive-portal, package, speed, time, data or device controls; spam; harassment; impersonation; or infringement of another person's rights.

Do not share access credentials, vouchers, passwords, one-time codes, M-PESA PINs or support-session tokens. Do not upload executable files, scripts, archives containing executable content, or any attachment that may place users or platform systems at risk.

3. Network integrity

Do not connect equipment that interferes with the network, re-broadcast a service without approval, change router settings outside your authority, or expose router management services to the public internet. Integrated routers must use the signed, outbound JOJO CONNECT agent and the router-specific onboarding or repair instructions issued to the authorised workspace.

4. Enforcement

JOJO Technologies and the relevant authorised operator may investigate credible abuse, suspend or limit access, quarantine unsafe uploads, preserve appropriate evidence, and cooperate with lawful requests where required. Action will be proportionate to the risk, evidence and applicable law.

5. Reporting concerns

Report suspected misuse, a lost device, a compromised account or a security concern promptly to support@jojotech.co.ke. Do not include passwords, M-PESA PINs or one-time codes in a report.