



5th Generation Networks (Pty) Ltd

Reg: 2019/108057/07 | ICASA License: CECS-E/0033/2024

ACCEPTABLE USE POLICY

Governing the responsible and lawful use of fibre internet services delivered over the Openserve network

Effective Date: 24 June 2026

Version 1.0

IMPORTANT NOTICE: This Acceptable Use Policy ("AUP") forms part of your Service Agreement and Terms and Conditions of Service with 5th Generation Networks (Pty) Ltd. By subscribing to or using our services, you agree to comply with this AUP in full. Failure to comply may result in suspension, restriction, or termination of services.

1. PURPOSE

This Acceptable Use Policy ("AUP") governs the use of all services, networks, infrastructure, systems, applications, and equipment provided by 5th Generation Networks (Pty) Ltd ("5th Generation Networks", "we", "us", or "our").

All Customers, Subscribers, Users, and any persons making use of our services ("Customer" or "User") agree to comply with this AUP when accessing or using any services provided by 5th Generation Networks.

Failure to comply with this policy may result in suspension, restriction, or termination of services.

2. COMPLIANCE WITH LAWS

2.1 Lawful Use

Services may only be used for lawful purposes and in accordance with the laws of the Republic of South Africa.

Users must comply with all applicable legislation, including but not limited to:

- Electronic Communications Act 36 of 2005
- Electronic Communications and Transactions Act 25 of 2002
- Consumer Protection Act 68 of 2008
- Cybercrimes Act 19 of 2020
- Protection of Personal Information Act 4 of 2013 (POPIA)
- Films and Publications Act



- Copyright Act 98 of 1978
- Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA)

2.2 Illegal Content

Users may not transmit, distribute, store, publish, or make available content that:

- Is unlawful or prohibited by legislation;
- Contains child sexual abuse material (CSAM);
- Constitutes hate speech or incitement to violence;
- Is defamatory, threatening, fraudulent, or misleading;
- Infringes copyright, trademark, patents, or other intellectual property rights;
- Violates privacy rights or data protection laws.

3. NETWORK USAGE

3.1 Internet Content

5th Generation Networks does not control information available on the Internet and accepts no responsibility for the content of websites, emails, applications, or online services accessed by Customers. Users access Internet content entirely at their own risk.

3.2 Third-Party Networks

Our services provide access to networks operated by third parties, including Openserve as our Fibre Network Operator (FNO). Customers must comply with the acceptable use policies and terms of those networks and services.

3.3 Copyrighted Material

Users may download copyrighted material only where legally permitted. The unauthorized distribution, reproduction, sharing, or transmission of copyrighted content is prohibited.

4. PROHIBITED ACTIVITIES

Users may not use our services to engage in the following:

4.1 Fraud and Criminal Activity

- Commit fraud;
- Engage in identity theft;
- Conduct phishing attacks;
- Distribute malicious software;
- Facilitate financial crimes.



4.2 Cybersecurity Violations

- Hacking or unauthorised access to systems or networks;
- Password attacks or brute-force attempts;
- Vulnerability scanning without authorisation;
- Network intrusion or exploitation of security weaknesses;
- Deploying malware, ransomware, spyware, or trojans.

4.3 Denial of Service Attacks

- Conducting DDoS or denial-of-service attacks;
- Flooding networks, systems, or servers;
- Intentionally degrading network performance for other users.

4.4 Spoofing

The forging or alteration of email headers, packet headers, source addresses, or domain identities is strictly prohibited.

4.5 Circumvention

Users may not attempt to bypass security controls, usage restrictions, network management systems, authentication mechanisms, or service limitations implemented by 5th Generation Networks.

5. SYSTEM AND NETWORK SECURITY

Users may not:

- Gain unauthorised access to any system or network;
- Probe or scan networks without permission;
- Monitor network traffic unlawfully;
- Interfere with services used by others;
- Attempt to compromise network integrity.

5th Generation Networks reserves the right to investigate suspected security incidents and cooperate with law enforcement authorities where criminal activity is suspected.

6. FAIR USE AND NETWORK MANAGEMENT

6.1 Fair Usage

To ensure equitable access for all Customers, 5th Generation Networks reserves the right to implement reasonable network management practices in accordance with ICASA's Open Access requirements. These may include:

- Traffic prioritisation;
- Traffic shaping;
- Throughput management;
- Congestion management;



- Temporary service limitations.

6.2 Excessive Usage

Where usage materially affects network performance or negatively impacts other users, we may:

- Reduce service throughput;
- Restrict certain applications or protocols;
- Temporarily suspend services;
- Require migration to a more suitable package;
- Terminate services for repeated abuse.

6.3 Malicious Traffic

Traffic generated by viruses, worms, malware, botnets, or compromised devices may be blocked, filtered, or restricted to protect the integrity of the network. Customers are responsible for securing their own equipment.

7. EMAIL AND MESSAGING SERVICES

Users may not:

- Send unsolicited bulk email ("spam");
- Send chain letters;
- Conduct email bombing attacks;
- Distribute malware through email;
- Use misleading email headers;
- Operate open mail relays.

Where mail services are provided, Customers are responsible for maintaining adequate security on their mail servers and ensuring compliance with ECTA and POPIA.

8. RESALE OF SERVICES

Customers may not resell services, share commercial services, or provide Internet access to third parties for compensation without the prior written consent of 5th Generation Networks.

Authorised resellers remain responsible for the conduct of their users and must ensure their own end-users comply with this AUP.

9. CUSTOMER EQUIPMENT

Customers remain responsible for:

- Securing routers and Wi-Fi networks;
- Maintaining strong passwords and access controls;
- Keeping firmware and software updated;
- Protecting all connected devices from malware.



Compromised equipment generating malicious traffic may be disconnected from the network until the issue has been resolved to 5th Generation Networks' satisfaction.

10. PRIVACY AND MONITORING

5th Generation Networks respects Customer privacy and processes personal information in compliance with the Protection of Personal Information Act (POPIA). We may monitor network traffic metadata, usage statistics, security events, and performance information for the purposes of:

- Network management;
- Security and fraud prevention;
- Service optimisation;
- Compliance with legal obligations.

We do not monitor the content of communications except where required by law in accordance with RICA. For data-related queries or to exercise your POPIA rights, contact our Information Officer at Rinaldo@5thgennetworks.co.za.

11. REPORTING ABUSE

Customers are encouraged to report violations of this AUP. All reports will be investigated in confidence. Reports should include the date and time of the incident, source IP addresses, relevant logs or evidence, and a description of the activity.

Channel	Details
General Support	info@5thgennetworks.co.za
Abuse / Compliance	Rinaldo@5thgennetworks.co.za
Telephone	+27 69 509 9995
Physical Address	Highgrove Office Park, 50 Tegel Avenue, Highveld Centurion
Website	www.5thgennetworks.co.za

12. VIOLATIONS AND ENFORCEMENT

Upon becoming aware of an alleged violation, 5th Generation Networks may take one or more of the following actions at its sole and absolute discretion:

- Issue a warning to the User;
- Restrict or rate-limit services;
- Suspend services temporarily pending investigation;
- Terminate services with immediate effect;
- Remove or block offending content or traffic;
- Report incidents to ICASA, SAPS, cybercrime investigators, or relevant regulatory bodies;
- Pursue civil action to recover damages, administrative costs, investigation expenses, and legal fees.



The taking of any one of the steps above does not preclude the concurrent or subsequent taking of any other step.

13. CHANGES TO THIS POLICY

5th Generation Networks reserves the right to amend this Acceptable Use Policy at any time. Updated versions will be published on our website at www.5thgennetworks.co.za and customers will be notified by email at least thirty (30) calendar days before material amendments take effect.

Continued use of our services after publication of a revised policy constitutes acceptance of that revised policy.

14. CONTACT DETAILS

For all enquiries relating to this AUP, please contact 5th Generation Networks using the details below:

5th Generation Networks (Pty) Ltd	Highgrove Office Park, 50 Tegel Avenue, Highveld Centurion
Telephone	+27 69 509 9995
General Email	info@5thgennetworks.co.za
Abuse Reports	Rinaldo@5thgennetworks.co.za
Website	www.5thgennetworks.co.za
Reg Number	2019/108057/07
ICASA License	CECS-E/0033/2024

DOCUMENT APPROVAL

Field	Details	Status
Document	Acceptable Use Policy (AUP)	Final
Version	1.0	Approved
Effective Date	23 June 2026	Active
Approved By	5th Generation Networks Management	✓ Approved
Next Review	June 2027	Scheduled

5th Generation Networks (Pty) Ltd | Reg: 2019/108057/07 | ICASA: CECS-E/0033/2024 | info@5thgennetworks.co.za | +27 69 509 9995 | www.5thgennetworks.co.za