



Acceptable Use Policy (AUP)

Version Date: 022026

1. Purpose

This Acceptable Use Policy ("Policy") sets out the rules governing use of services provided by NetlinQ UK UK Ltd ("NetlinQ UK", "we", "us", "our"). This Policy applies to all broadband, leased line, VoIP, mobile, hosted and related connectivity services supplied by NetlinQ UK. By using our services, the Customer agrees to comply with this Policy.

2. Lawful Use

Customers must use all services lawfully and in accordance with applicable UK laws and regulations. The Customer must not use the services for:

- Any unlawful, fraudulent, or criminal activity
- Distribution of malware, viruses or malicious software
- Copyright infringement or unauthorised distribution of protected content
- Harassment, abuse or threatening communications
- Transmission of unlawful, defamatory or offensive material

3. Network Integrity & Fair Usage

Customers must not use the services in a way that damages, disrupts or degrades network performance, adversely affects other users, places excessive or abnormal load on the network, or circumvents technical safeguards or security measures.

Where "unlimited" services are supplied, usage must remain consistent with normal business activity and must not compromise network stability.

4. VoIP & Telephony Services

The Customer must not:

- Conduct nuisance or unsolicited calling campaigns
- Use automated dialling systems without prior agreement
- Engage in CLI spoofing or call masking for deceptive purposes
- Generate fraudulent traffic, including premium rate abuse
- Use services for bulk SMS or messaging platforms without agreement

NetlinQ UK reserves the right to suspend services where unusual call patterns or suspected fraud is detected.

5. Mobile Services

Mobile SIMs supplied by NetlinQ UK must not be used for:

- Bulk messaging or SMS aggregation platforms
- Grey routing or international bypass services
- Unauthorised resale
- Permanent roaming outside permitted territories

Usage must comply with upstream carrier rules.

6. Hosting & Internet Services

Customers must not:

- Host illegal content
- Operate open relays or unsecured servers
- Facilitate denial of service (DoS/DDoS) attacks
- Engage in phishing or impersonation schemes

7. Security & Customer Responsibilities

Customers are responsible for securing their own equipment and passwords, ensuring internal users comply with this Policy, and promptly notifying NetlinQ UK of suspected breaches or security incidents.

8. Monitoring & Enforcement

NetlinQ UK may monitor network usage to ensure compliance with this Policy and upstream carrier obligations.

Where a breach is suspected, NetlinQ UK may:

- Issue a warning
- Restrict or suspend services
- Terminate services in serious or repeated cases
- Report matters to relevant authorities where required by law

Suspension may occur without notice where immediate action is required to protect network integrity or comply with legal obligations.

9. Liability

NetlinQ UK shall not be liable for losses arising from suspension or restriction of services where action is taken in accordance with this Policy.

10. Amendments

NetlinQ UK may update this Policy from time to time. The latest version will be made available upon request or published on our website.