

ACCEPTABLE USE POLICY (AUP)

Firstcom Europe Ltd Version: 2026.1 — Effective from: 01/08/2026

This Acceptable Use Policy (“AUP”) forms part of the Agreement between Firstcom Europe Ltd (“Firstcom”) and the Customer. It sets out the rules governing the Customer’s use of Firstcom’s telecoms, connectivity, hosted voice, IT services, and any associated equipment.

The purpose of this AUP is to ensure the integrity, security, and lawful use of Firstcom’s network and services.

1. GENERAL PRINCIPLES

The Customer must use Firstcom’s services in a lawful, responsible, and reasonable manner. The Customer must not use the services in any way that:

- Causes disruption to Firstcom’s network
- Harms other users
- Violates applicable laws or regulations
- Exposes Firstcom to legal or reputational risk

The Customer is responsible for all use of the services by its employees, contractors, and end-users.

2. PROHIBITED ACTIVITIES

The Customer must not use Firstcom’s services to:

2.1 Illegal or Unlawful Activity

- Commit or facilitate fraud
- Access or distribute illegal content
- Infringe intellectual property rights
- Engage in harassment, threats, or abuse
- Conduct unauthorised surveillance or interception of communications

2.2 Network Misuse

- Attempt to bypass security controls
- Interfere with network performance
- Launch or participate in DDoS attacks
- Spread malware, viruses, or malicious code
- Perform unauthorised penetration testing or scanning

2.3 Misuse of Telecoms Services

- Make automated or artificially generated traffic (AGT)
- Use auto-diallers, predictive diallers, or dialling robots without written consent
- Generate excessive or abnormal call patterns
- Manipulate CLI or present unauthorised numbers
- Use services for telemarketing without appropriate licences

2.4 Misuse of IT Services

- Install unlicensed or illegal software
- Disable or tamper with security tools deployed by Firstcom
- Circumvent monitoring or management agents
- Store prohibited, harmful, or unlawful data on managed systems

3. EMAIL & INTERNET USE (WHERE PROVIDED)

The Customer must not use Firstcom-provided email or internet services to:

- Send spam or unsolicited bulk messages
- Distribute harmful or offensive material
- Host or distribute copyrighted material without permission
- Operate public-facing services (e.g., web servers) unless authorised

4. SECURITY REQUIREMENTS

The Customer must:

- Maintain strong passwords and access controls
- Keep devices patched and updated
- Ensure anti-virus/EDR is active where required
- Notify Firstcom immediately of suspected security incidents
- Not share administrative credentials with unauthorised persons

If the Customer's security practices pose a risk to the network, Firstcom may require corrective action.

5. FAIR USAGE

Where services include “unlimited” or “fair usage” terms, the Customer must use the service in a manner consistent with normal business use.

Firstcom may apply traffic management, restrictions, or additional charges if usage is:

- Excessive
- Abnormal
- Disproportionate compared to typical business usage
- Causing network degradation

5.1 Voice Services

To ensure network stability and prevent misuse, the following Fair Usage limits apply to inclusive call bundles:

- **2,000 minutes per user per month** (landline and mobile destinations combined)
- Excess usage may be charged at the standard out-of-bundle rate
- Firstcom reserves the right to investigate abnormal or excessive call patterns

5.2 Connectivity Services

Broadband and connectivity services are provided on a Fair Usage basis. The following thresholds apply:

- **FTTP / SoGEA / Broadband:** Up to **2 TB per month** per circuit
- **Ethernet / Leased Line:** Up to **10 TB per month** per circuit

Usage significantly above these thresholds may result in:

- Traffic management
- Additional charges
- A requirement to upgrade to a higher-capacity service

6. VOICE FRAUD & MISUSE

The Customer must take reasonable steps to secure their PBX, handsets, routers, and network.

The Customer is responsible for:

- Toll fraud arising from insecure equipment
- Unauthorised access to their systems
- Costs incurred due to compromised devices

Firstcom may temporarily suspend outbound calling if fraud is suspected.

7. SUSPENSION OF SERVICE

Firstcom may suspend or restrict services without liability if:

- The Customer breaches this AUP
- The Customer's usage threatens network stability
- Required by law enforcement or regulatory bodies
- Fraud or security compromise is suspected

Where reasonable, Firstcom will notify the Customer before suspension.

8. CUSTOMER RESPONSIBILITY FOR USERS

The Customer is responsible for ensuring that all employees, contractors, and end-users comply with this AUP.

Failure by any user is treated as a failure by the Customer.

9. CHANGES TO THIS POLICY

Firstcom may update this AUP from time to time to reflect:

- Legal or regulatory changes
- Network or service updates
- Security requirements

Updated versions will be published or provided to the Customer.

10. CONTACT

For questions regarding this AUP, the Customer may contact:

Firstcom Europe Ltd 1b Parklands, Bolton, BL6 4SD – fauls@firstcomeurope.co.uk –

0333 023 7000

END OF AUP