

NEXLINK COMMUNICATIONS INC.

Acceptable Use Policy

What you may and may not do with your NexLink connection.

Document	Version	Effective	Review by
NX-AUP-001	Interim 1.0	10 July 2026	10 July 2027

◆ **NOTE** *Interim version, in force from 10 July 2026. Adopted for immediate use and pending review by NexLink's attorney; terms may be updated. This document reflects generally accepted WISP practice and the Guyana Data Protection Act 2023. The current version is always at nexlinkonline.com.*

1. Purpose

This Acceptable Use Policy ("AUP") protects our network, our other customers, and the public. It applies to everyone who uses a NexLink Communications Inc. connection, whether or not they are the account holder. By using the Service you agree to it.

1.1 This AUP forms part of your Customer Terms & Conditions. Where the two differ on a matter of acceptable use, this AUP prevails.

2. Lawful use

You must not use the Service to do anything unlawful under the laws of Guyana, or to help anyone else do so. This includes, without limitation:

- Accessing, storing, or distributing child sexual abuse material. We report such activity to the Guyana Police Force without notice.
- Fraud, phishing, identity theft, or financial crime.
- Distributing material that is defamatory, or that unlawfully incites violence or hatred.
- Infringing copyright, trademarks, or other intellectual property, including unlicensed distribution of films, music, or software.
- Breaching the Cyber Crime Act or the Telecommunications Act.

◆ **NOTE** *Interim default value, adopted for immediate use and subject to legal review.*

3. Network integrity and security

You must not use the Service to:

- Gain or attempt unauthorised access to any system, network, or account ("hacking").
- Distribute malware, ransomware, viruses, or other harmful code.
- Launch or participate in denial-of-service attacks.
- Scan, probe, or test the vulnerability of any network without authorisation.

- Forge headers or otherwise falsify the origin of any transmission, including email.
 - Circumvent any limits, authentication, or security we or others put in place.
- 3.1** You must secure your own equipment and Wi-Fi. An open or compromised network on your premises that is used to breach this AUP is your responsibility.

4. Email and messaging

- Do not send bulk unsolicited messages ("spam"), whether commercial or not.
- Do not operate open mail relays or open proxies.
- Do not harvest addresses or run mailing lists without consent.

5. Fair use and network capacity

Residential plans are for ordinary household use and are sold on a shared (contended) basis. They are not intended to carry sustained commercial-grade traffic.

- 5.1** You must not run a service on a residential plan that materially degrades the experience of other users on the same tower — for example, a high-traffic public server, a commercial Wi-Fi hotspot resold to others, or continuous high-volume seeding.
- 5.2** If your usage on a residential plan is so far outside normal household patterns that it harms others, we may contact you, ask you to move to a business plan, or apply the network management measures described in our Network Management & Traffic Practices disclosure. **We do not impose data caps and do not throttle by volume.**
- 5.3** Reselling the Service, or sharing it beyond your premises, requires a business plan and our written agreement.

6. Prohibited equipment and interference

- Do not connect equipment that interferes with our radio network or the licensed spectrum we use.
- Do not tamper with, move, or modify the radio, antenna, or PoE equipment we install.
- Do not attach unauthorised amplifiers or antennas to our equipment.

7. Consequences of breach

- 7.1** Where practical and lawful, we will contact you first and give you a chance to fix the problem.
- 7.2** For serious breaches — anything unlawful, any threat to network integrity, or anything endangering others — we may suspend or terminate the Service **immediately and without notice.**
- 7.3** We may report unlawful activity to the authorities and preserve relevant records for them, in accordance with our Privacy Notice and applicable law.
- 7.4** Suspension for breach does not entitle you to a service credit or refund, and does not pause your billing unless we say so in writing.

8. Reporting abuse

Report abuse of our network — spam, hacking, or illegal content originating from a NexLink connection — to support@nexlinkonline.com. We investigate every credible report.

9. Changes

We may update this AUP to address new threats or legal requirements. The current version is always available at nexlinkonline.com. Continued use after a change means you accept it.