(AUP)
ACCEPTABLE USE POLICY

Version: 03.2026

PureLink

ACCEPTABLE USE POLICY (AUP)

This Acceptable Use Policy ("AUP") forms part of the Agreement between the Service Provider and the Client and is subject to the Master Internet Service Terms ("Master Terms). Capitalised terms have the meaning given in the Master Terms.

1. PURPOSE OF THIS AUP

1.1 Purpose

The AUP ensures:
(a) protection of the Network;
(b) fair access for all users;
(c) compliance with New Zealand law;
(d) compliance with Supplier policies.

1.2 Responsibility for End Users

You are responsible for all use of the Services, including use by your employees, contractors, household members, or other end users. Any breach of this AUP by an end user is deemed to be a breach by you.

2. PROHIBITED ACTIVITIES

You must not use the Services to:

2.1 Illegal or harmful activity

(a) break any law;
(b) host or distribute illegal content;
(c) engage in fraud, identity theft, or scams.

2.2 Network abuse

(a) interfere with, disrupt, or degrade the Network;
(b) perform denial-of-service attacks;
(c) probe, scan, or test network security without permission;
(d) circumvent firewalls or CG-NAT;
(e) attempt to bypass traffic management controls.

2.3 Email & messaging abuse

(a) send unsolicited bulk email;
(b) operate open SMTP relays;
(c) send malware, phishing or harmful links;
(d) generate excessive SMTP traffic inconsistent with normal use.

2.4 Hosting & server restrictions

(a) run public-facing servers on residential plans;

(b) host PBX, SIP servers, web servers, mail servers, game servers or similar on residential plans;
(c) operate any service likely to attract denial-of-service activity.

2.5 IP addressing abuse
(a) use IP addresses inconsistently with allocation;
(b) attempt to modify or spoof IP addresses;
(c) exceed assigned address ranges.

2.6 High-risk behaviour
(a) violate Supplier AUPs;
(b) overload international transit;
(c) engage in sustained high-volume usage impacting others.

2.7 Prohibited Content

You must not use the Services to access, store, transmit or distribute content that is:

(a) objectionable, restricted, or prohibited under New Zealand law (including classifications under the Films, Videos, and Publications Classification Act 1993);
(b) defamatory, hateful, abusive, or inciting violence;
(c) sexually explicit material involving minors, exploitation, or non-consensual imagery;
(d) malicious software, harmful code, or tools designed for compromising security;
(e) content that infringes privacy rights, including doxxing or unauthorised disclosure of personal information;
(f) content that promotes self-harm, violence, or criminal activity; or
(g) otherwise harmful to the Network or inconsistent with reasonable community standards.

2.8 Copyright & Intellectual Property

You must not use the Services to upload, share, download, host, or distribute any content that infringes copyright or other intellectual property rights. This includes (without limitation):
(a) sharing or downloading copyrighted material without permission (e.g., movies, TV shows, software, games);
(b) using peer-to-peer or file-sharing applications for unauthorised distribution;
(c) bypassing digital rights management (DRM) restrictions; or
(d) using the Network to facilitate or conceal copyright infringement by others.

You are responsible for ensuring you have the necessary rights or licences for any content you use or share via the Services.

3. SECURITY OBLIGATIONS

You must:

3.1 maintain secure passwords and access controls;
3.2 patch and maintain your own devices;
3.3 secure your internal network;
3.4 notify us of any suspected breach.

4. RESIDENTIAL VS BUSINESS USE

4.1 Residential plans are not designed for:
(a) commercial hosting;
(b) enterprise workloads;
(c) high-availability requirements;
(d) running an office network.

4.2 Business plans may permit server hosting if permitted by the Order.

5. ENFORCEMENT & REMEDIES

We may:
5.1 investigate suspected breaches;
5.2 request information from you;
5.3 suspend or restrict the Service;
5.4 implement shaping or traffic management;
5.5 remove harmful traffic;
5.6 terminate the Service in accordance with the Master Terms.

5.7 Monitoring and Legal Compliance
We do not monitor your content, but we may act on complaints or suspected breaches. We may cooperate with law enforcement agencies, emergency services, or other network operators where legally required or where necessary to protect the Network.

6. CHANGES TO THIS AUP

We may update this AUP by publishing an updated version here. Changes will be managed in accordance with clause 19.5 of the Master Terms.

PureLink

www.purelink.nz

help@purelink.nz

0800 100 714

Follow us on LinkedIn