Northland Communications

Internet Acceptable Use Policy

Revision 05.04.22

1. Introduction

This Acceptable Use Policy (AUP) specifies actions prohibited by Northland Communications. Northland Communications retains the right to modify the Acceptable Use Policy at any time, with or without any notification, and any such modification shall be automatically effective as to all customers when adopted by Northland. Questions or comments regarding the Acceptable Use Policy should be forwarded to policy@northland.net.

2. Non-Monitoring Notice

Corporate Disclaimer: Northland Communications' customers and users should be aware that Northland Communications does not exercise any editorial control over, set standards for, or monitor the contents of any message which appears on, or is accessed through Northland Communications service, the "Internet", any electronic bulletin board or "web site", or any electronic information service. Responsibility for accuracy, suitability, and standards of all such messages rests solely with the originators and recipients of such messages.

3. Compliance with Law

Customer shall not post, transmit, re-transmit or store material on or through any of Services or Products which, in the sole judgment of the Company (i) is in violation of any local, state, federal or non-United States law or regulation, (ii) threatening, obscene, indecent, defamatory or that otherwise could adversely affect any individual, group or entity (collectively, "Persons") or (iii) violates the rights of any person, including rights protected by copyright, trade secret, patent or other intellectual property or similar laws or regulations including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Customer. Customer shall be responsible for determining what laws or regulations are applicable to its use of the Services and Products

3.1. Transmission or Dissemination of Child Pornography

Northland Communications' network may not be used by customers in any fashion for the transmission or dissemination of images containing child pornography. Northland Communications receives all complaints, including complaints that may concern child pornography through the following email addresses: abuse@northland.net or abuse-cp@northland.net

4. Prohibited Use of Services and Products

4.1. General

4.1.1 Resale of Services and Products, without the prior consent of the Company 4.1.2 Deceptive Online marketing practices (i.e. Spam). 4.1.3 Violations of the rights of any Person protected by copyright, trade secret, patent or other intellectual

property or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Customer. 4.1.4. Actions that restrict or inhibit any Person, whether a customer of the Company or otherwise, in its use or enjoyment of any of the Company's Services or Products.

4.2. Email

4.2.1 Sending unsolicited bulk or commercial messages ("spam").

This includes, but is not limited to, bulk mailing of commercial advertising, informational announcements, charity requests, petitions for signatures, and political or religious tracts. Such messages may only be sent to those who have explicitly requested it.

4.2.2 Collecting responses from unsolicited bulk or commercial e-mail sent from accounts with other providers.

4.2.3 Sending Unsolicited Commercial Email from Northland Communications or from another provider to advertise any service that is hosted by Northland Communications or connected via Northland Communications.

4.2.4 Creating or forwarding "chain letters" or other "pyramid schemes" of any type.

4.2.5. Harassment, whether through language, frequency of messages, or size of messages.

4.2.6 Collecting replies to messages sent from another Internet service provider if those messages violate this Acceptable Use Policy or the acceptable use policy of the other service provider.

4.2.7 Intentionally distributing computer viruses, worms or any computer program or message with the intent of causing harm to the recipient's computer system or network.

4.2.8 Deceptively forging Email headers or providing false information to deceive the recipient or redirect replies to a non-existent Email address.

4.2.9 Using the Email system of a third party without authorization with the intent to send unsolicited mass Email or to cause harm to third party systems.

4.3. System and Network

4.3.1 Unauthorized access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of a system or network or to breach

security or authentication measures without express authorization of the owner of the system or network.

4.3.2 Performing any action that disrupts Internet access for another user or interferes with Internet communications, including, but not limited to, port scanning, ping flooding, nuking, packet spoofing or any denial of service method.
4.3.3 Unauthorized monitoring of data or traffic on any network or system without express authorization of the owner of the system or network. 4.3.4 Attempting to forge any TCP-IP packet header with malicious intent.