

Douglas Fast Net Acceptable Use Policy

Introduction

Douglas Fast Net (DFN) is at all times committed to complying with the laws and regulations governing use of the Internet, e-mail transmission and text messaging and preserving for all of its Customers the ability to use DFN's network and the Internet without interference or harassment from other users. The DFN Acceptable Use Policy ("AUP") is designed to help achieve these goals.

By using IP Services, as defined below, Customer agrees to comply with this Acceptable Use Policy and to remain responsible for its users. DFN reserves the right to change or modify the terms of the AUP at any time, effective when posted on DFN's web site at www.dfn.net/acceptable-use-policy. Customer's use of the IP Service after changes to the AUP are posted shall constitute acceptance of any changed or additional terms.

As used in this AUP, the term "Customer" refers to the person or entity of record as responsible for the subscription to IP Services and can refer to more than one person or entity, where appropriate and also includes any person or entity using Customer's IP Services.

Scope of the AUP

The AUP applies to the DFN services that provide (or include) access to the Internet, including hosting services (software applications and hardware), or are provided over the Internet or wireless data networks (collectively "IP Services").

Prohibited Activities

General Prohibitions:

DFN prohibits use of the IP Services in any way that is unlawful, harmful to or interferes with use of DFN's network or systems, or the network of any other provider, interferes with the use or enjoyment of services received by others, infringes intellectual property rights, results in the publication of threatening or offensive material, or constitutes Spam/E-mail/Usenet abuse, a security risk or a violation of privacy.

Customer is responsible for any misuse of IP Services that originates from Customer's account, even activities committed by a friend, family member, co-worker, employee, guest or anyone with access to the account. Customer is responsible to ensure that others do not gain unauthorized access to the IP Services.

Customer may not resell the IP Services without the express written consent of DFN, which may be granted or withheld in DFN's sole discretion.

Unlawful Activities:

IP Services shall not be used in connection with any criminal, civil or administrative violation of any applicable local, state, provincial, federal, national or international law, treaty, court order, ordinance, regulation or administrative rule.

Violation of Intellectual Property Rights:

IP Services shall not be used to publish, submit/receive, upload/download, post, use, copy or otherwise reproduce, transmit, re-transmit, distribute or store any content/material or to engage in any activity that infringes, misappropriates or otherwise violates the intellectual property rights or privacy or publicity rights of DFN or any individual, group or entity, including but not limited to any rights protected by any copyright, patent, trademark laws, trade secret, trade dress, right of privacy, right of publicity, or other intellectual property right now known or later recognized by statute, judicial decision or regulation.

Threatening Material or Content:

IP Services shall not be used to host, post, transmit, or re-transmit any content or material (or to create a domain name or operate from a domain name), that harasses, or threatens the health or safety of others. In addition, for those IP Services that utilize DFN provided web hosting, DFN reserves the right to decline to provide such services if

the content is determined by DFN to be obscene, indecent, hateful, malicious, racist, defamatory, fraudulent, libelous, treasonous, excessively violent or promoting the use of violence or otherwise harmful to others.

Inappropriate Interaction with Minors:

DFN complies with all applicable laws pertaining to the protection of minors, including when appropriate, reporting cases of child exploitation to the National Center for Missing and Exploited Children. For more information about online safety, visit www.ncmec.org.

Child Pornography:

IP Services shall not be used to publish, submit/receive, upload/download, post, use, copy or otherwise produce, transmit, distribute or store child pornography. Suspected violations of this prohibition may be reported to DFN at the following e-mail address: abuse@douglasfast.net. DFN will report any discovered violation of this prohibition to the National Center for Missing and Exploited Children and/or law enforcement agencies and take steps to remove child pornography (or otherwise block access to the content determined to contain child pornography) from its servers.

Spam/E-mail/Usenet Abuse:

Violation of the CAN-SPAM Act of 2003, or any other applicable law regulating e-mail services, constitutes a violation of this AUP.

Spam/E-mail or Usenet abuse is prohibited using IP Services. Examples of Spam/E-mail or Usenet abuse include but are not limited to the following activities:

- sending multiple unsolicited electronic mail messages or "mail-bombing" – to one or more recipient;
- sending unsolicited commercial e-mail, or unsolicited electronic messages directed primarily at the advertising or promotion of products or services;
- sending unsolicited electronic messages with petitions for signatures or requests for charitable donations, or sending any chain mail related materials;
- sending bulk electronic messages without identifying, within the message, a reasonable means of opting out from receiving additional messages from the sender;
- sending electronic messages, files or other transmissions that exceed contracted for capacity or that create the potential for disruption of the DFN network or of the networks with which DFN interconnects, by virtue of quantity, size or otherwise;
- using another site's mail server to relay mail without the express permission of that site;
- using another computer, without authorization, to send multiple e-mail messages or to retransmit e-mail messages for the purpose of misleading recipients as to the origin or to conduct any of the activities prohibited by this AUP;
- using IP addresses that the Customer does not have a right to use;
- collecting the responses from unsolicited electronic messages;
- maintaining a site that is advertised via unsolicited electronic messages, regardless of the origin of the unsolicited electronic messages;
- sending messages that are harassing or malicious, or otherwise could reasonably be predicted to interfere with another party's quiet enjoyment of the IP Services or the Internet (e.g., through language, frequency, size or otherwise);
- using distribution lists containing addresses that include those who have opted out;
- sending electronic messages that do not accurately identify the sender, the sender's return address, the e-mail address of origin, or other information contained in the subject line or header;
- falsifying packet header, sender, or user information whether in whole or in part to mask the identity of the sender, originator or point of origin;
- using redirect links in unsolicited commercial e-mail to advertise a website or service;
- posting a message to more than ten (10) online forums or newsgroups, that could reasonably be expected to generate complaints;
- intercepting, redirecting or otherwise interfering or attempting to interfere with e-mail intended for third parties;

- knowingly deleting any author attributions, legal notices or proprietary designations or labels in a file that the user mails or sends;
- using, distributing, advertising, transmitting, or otherwise making available any software program, product, or service that is designed to violate this AUP or the AUP of any other Internet Service Provider, including, but not limited to, the facilitation of the means to spam.

Security Violations

Customer is responsible for ensuring and maintaining security of its systems and the machines that connect to and use IP Service(s), including implementation of necessary patches and operating system updates. Due to the public nature of the Internet, all email is considered to be publicly accessible and important information should be treated carefully. DFN is not liable for the protection or maintenance of privacy of email or other information transferred through the Internet. Customer is solely responsible for protection of Customer's identity from identity theft.

IP Services may not be used to interfere with, gain unauthorized access to, or otherwise violate the security of DFN's (or another party's) server, network, network access, personal computer or control devices, software or data, or other system, or to attempt to do any of the foregoing. Examples of system or network security violations include but are not limited to:

- unauthorized monitoring, scanning or probing of network or system or any other action aimed at the unauthorized interception of data or harvesting of email addresses;
- hacking, attacking, gaining access to, breaching, circumventing or testing the vulnerability of the user authentication or security of any host, network, server, personal computer, network access and control devices, software or data without express authorization of the owner of the system or network;
- impersonating others or secretly or deceptively obtaining personal information of third parties (phishing, etc.);
- using any program, file, script, command or transmission of any message or content of any kind, designed to interfere with a terminal session, the access to or use of the Internet or any other means of communication;
- distributing or using tools designed to compromise security (including but not limited to SNMP tools), including cracking tools, password guessing programs, packet sniffers or network probing tools (except in the case of authorized legitimate network security operations);
- knowingly uploading or distributing files that contain viruses, spyware, Trojan horses, worms, time bombs, cancel bots, corrupted files, root kits or any other similar software or programs that may damage the operation of another's computer, network system or other property, or be used to engage in modem or system hijacking;
- engaging in the transmission of pirated software;
- with respect to dial-up accounts, using any software or device designed to defeat system time-out limits or to allow Customer's account to stay logged on while Customer is not actively using the IP Services or using such account for the purpose of operating a server of any type;
- using manual or automated means to avoid any use limitations placed on the IP Services;
- providing guidance, information or assistance with respect to causing damage or security breach to DFN's network or systems, or to the network of any other IP Service provider;
- failure to take reasonable security precautions to help prevent violation(s) of this AUP.

Customer Responsibilities

Customer remains solely and fully responsible for the content of any material posted, hosted, downloaded/uploaded, created, accessed or transmitted using the IP Services. DFN has no responsibility for any material created on the DFN's network or accessible using IP Services, including content provided on third-party websites linked to the DFN network. Such third-party website links are provided as Internet navigation tools for informational purposes only, and do not constitute in any way an endorsement by DFN of the content(s) of such sites.

Customer is responsible for taking prompt corrective action(s) to remedy a violation of AUP and to help prevent similar future violations.

AUP Enforcement and Notice

Customer's failure to observe the guidelines set forth in this AUP may result in DFN taking actions anywhere from a warning to a suspension or termination of Customer's IP Services. When feasible and, in DFN's opinion, DFN may provide Customer with a notice of an AUP violation via e-mail or otherwise allowing the Customer to promptly correct such violation.

DFN reserves the right, however, to act immediately and without notice to suspend or terminate affected IP Services in response to a court order or government notice that certain conduct must be stopped, or when DFN reasonably determines that the Customer's use of the affected IP Services may: (1) expose DFN to sanctions, prosecution, civil action or any other liability; (2) cause harm to or interfere with the integrity or normal operations of DFN's network or networks with which DFN is interconnected; (3) interfere with another DFN Customer's use of IP Services or the Internet; (4) violate any applicable law, rule or regulation; or (5) otherwise present an imminent risk of harm to DFN or other DFN customers.

Any failure of DFN to take action in any instance shall not be construed to be a waiver of any right to do so in another instance.

Copyright Infringement & Digital Millennium Copyright Act

DFN respects the intellectual property rights of others. The Digital Millennium Copyright Act of 1998 (the "DMCA" found at 17 U.S.C. § 512) provides that owners of copyrighted works who believe that their rights under U.S. copyright law have been infringed may report alleged infringements to service providers like DFN. In accordance with the DMCA and other applicable laws, DFN maintains a policy that provides for the termination of IP Services, under appropriate circumstances, if Customer is found to be a repeat infringer and/or if Customer's IP Services are used repeatedly for infringement (the "Repeat Infringer Policy"). DFN may terminate IP Services at any time with or without notice to Customers.

DFN has no obligation to investigate possible copyright infringements with respect to materials transmitted by Customer or any other users of the IP Services. However, DFN will process valid notifications of claimed infringement under the DMCA, and continued receipt of infringement notifications for Customer's account will be used as a factor in determining whether Customer is a repeat infringer. In addition, DFN may voluntarily participate, on terms acceptable to DFN, in copyright alert and graduated response programs.

Incident Reporting

Any complaints (other than claims of copyright infringement) regarding violation of this AUP by a DFN Customer (or its user) should be directed to abuse@douglasfast.net. Where possible, include details that would assist DFN in investigating and resolving such complaint (e.g., expanded headers, IP addresses, a copy of the offending transmission and any log files).

DMCA Copyright Notifications:

Pursuant to 17 U.S.C. §§ 512(b)–(d), a copyright holder may send DFN a valid notification of claimed copyright infringement under the DMCA. DFN's designated agent to receive notifications of claimed infringement as described in DMCA subsection 512(c)(3) is:

Network Operations
Douglas Fast Net
2350 NW Aviation Drive
Roseburg, OR. 97470
E-mail: abuse@douglasfast.net

Due to the substantial volume of notifications of claimed infringement that DFN receives and processes, we are unable to accept notices of alleged copyright infringement via this designated agent or email address other than notifications of claimed infringement sent pursuant to Sections 512(b)–(d).

Contact Information:

Any notification that DFN sends to its Customers pursuant to this AUP will be sent via e-mail to the e-mail address on file with DFN, or may be in writing to Customer's address of record. It is Customer's responsibility to promptly notify DFN of any change of contact information.

Effective Date: August 28, 2017