

FRAMEWORK IT ACCEPTABLE USE POLICY

Framework IT, LLC ("FWC") 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 Clients the ability to use FWC's network and the Internet without interference or harassment from other users. The FWC Acceptable Use Policy ("AUP") is designed to help achieve these goals.

By using FWC's Managed Internet Services, Client agrees to comply with this Acceptable Use Policy and to remain responsible for its users. FWC reserves the right to change or modify the terms of the AUP at any time, effective when posted on FWC's web site at www.frameworkcommunications/aup. Client's use of the Service(s) after changes to the AUP are posted shall constitute acceptance of any changed or additional terms.

General Prohibitions:

FWC prohibits use of the Services in any way that is unlawful, harmful to or interferes with use of FWC'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.

Unlawful Activities:

The Service 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:

The Service 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 FWC 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, moral rights or other intellectual property right now known or later recognized by statute, judicial decision or regulation.

Threatening Material or Content:

The Service 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, if the Service is used to provide web hosting, FWC reserves the right to decline to provide such services if the content is determined by FWC 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:

FWC 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:

The Service 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 FWC at the

following e-mail address: helpdesk@frameworkcommunications.com. FWC will report any discovered violation of this prohibition to the National Center for Missing and Exploited Children 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 the Service. 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 FWC network or of the networks with which FWC 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 Client 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:

Clients are responsible for ensuring and maintaining security of their systems and the machines that connect to and use the Service, including implementation of necessary patches and operating system updates.

The Service may not be used to interfere with, gain unauthorized access to, or otherwise violate the security of FWC (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 e-mail 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 hi-jacking;
- 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 Client's account to stay logged on while Client is not actively using the Service 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 Service;
- providing guidance, information or assistance with respect to causing damage or security breach to AT&T's network or systems, or to the network of any other Service provider;
- failure to take reasonable security precautions to help prevent violation(s) of this AUP.

Client Responsibilities:

Client remains solely and fully responsible for the content of any material posted, hosted, downloaded/uploaded, created, accessed or transmitted using the Service. FWC has no responsibility for any material created on the FWC's network or accessible using the Service, including content provided on third-party websites linked to the FWC 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 FWC of the content(s) of such sites.

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

AUP Enforcement and Notice

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

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

Incident Reporting: Any complaints (other than claims of copyright or trademark infringement) regarding violation of this AUP by a FWC Client (or its user) should be directed to helpdesk@frameworkcommunications.com.

Copyright complaints: If Client believes that it or its user's work has been copied and posted, stored or transmitted using the Services in a way that constitutes copyright infringement, please submit a notification pursuant to the Digital Millennium Copyright Act ("DMCA") in accordance with the process detailed at www.frameworkcommunications.com/dmca, and directed to the designated agent listed below:

FWC's Designated Copyright Agent for notice of claims of copyright or trademark infringement on the sites can be reached as follows:

Email: helpdesk@frameworkcommunications.com

Phone: 312-265-8733 Extension 203

Mail: Framework IT, LLC
700 N Sacramento Blvd
Suite 101
Chicago Illinois 60612

Designated Agent: Ross Dolce, Manager of Security & Copyright Infringement

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