

# **Hosting Acceptable Use Policy**

ifPeople, Inc. ([www.ifpeople.net](http://www.ifpeople.net))  
Document last updated December 19, 2006

In order to completely fulfill your needs as our client (hereinafter "Customer") for reliable service and to meet the challenge of supporting the Internet as a diverse forum for free and open discussion and the dissemination of information, we as a responsible ifPeople, has certain legal, ethical and operational obligations. ifPeople, Inc. (hereinafter "Company," "we," "our" or "us") has created this Acceptable Use Policy in order to provide a clear understanding of the rules, regulations and restrictions regarding the use of our hosting services.

This document is not exhaustive and ifPeople reserves the right to modify it at any time, effective upon posting of the new version on <http://www.ifPeople.net/policies>. An unlisted activity that is illegal, irresponsible or disruptive may also be a violation of our AUP.

To protect the competing interests of Internet users and our clients, we enforce this Acceptable Use Policy (AUP). This AUP, has been established in the spirit of determining guidelines for our customers, to clarify their rights and responsibilities as Internet users and customers of our services. This AUP aims to clearly outline those activities that are harmful to the efficiency of our servers and which, according to our discretion, compromise our shared hosting environment. As a member of the Internet community, our Company, through this AUP, aims to prevent those activities that are either irresponsible or disruptive to the Internet activities of others. We also proscribe all those activities that fall outside the legal boundaries of acceptable Internet use and behaviors. For any of the activities outlined below, we reserve the right to take preventative or corrective action, at our discretion.

The use of Company services by our customers constitutes an acceptance of the terms laid out in this AUP. This AUP may be revised in the future, in order to better meet the needs of the changing Internet environment, the legal landscape in the United States and our customers' needs. The continued use of our services constitutes an acceptance of any new terms and conditions. We strongly encourage you to review this AUP periodically or whenever you are contemplating any new activity related to your account with our Company.

## **Violations**

Customers are said to be in violation of this AUP when they, their customers, affiliates and/or subsidiaries engage in any of the following proscribed activities:

1. Spamming refers to the act of sending, supporting, assisting, or commissioning the sending of, unsolicited commercial messages over the Internet to others. 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 individuals that have explicitly requested the information from you. Spamming is considered harmful because it can overload the Company's server network, can disrupt service to our other customers, violate our terms of service with "upstream providers," and foster a negative perception toward the Company. Spamming includes, but is not limited to, any means of Internet-based transmissions, such as email, newsgroup, Internet fax or Internet phone. It is a violation of this AUP to commission spamming by a third-party, even if that third-party does not use Company systems, networks or resources, if the spam message contains any reference to a website hosted by us or contains any other reference, message or link attributable to any service, network or system of the Company.
2. Forging Headers refers to the act of altering, removing or misrepresenting email headers, whether in whole or in part, to mask the originator of the email. Like spam, forging headers is harmful to our servers and compromises our reputation.
3. Spamming Newsgroups by sending, or commissioning the sending of, commercial advertisements or other messages to one or more different, off-topic newsgroups, are unwelcome in most Usenet discussion groups and on most electronic mailing lists (discussion lists). If you are unsure about a posting to a Usenet group, please refer to the newsgroup or mailing list's charter to determine if advertising is allowed.
4. Harassment represents the act or intention of intimidating, threatening, frightening or otherwise

harassing others, using company servers, networks and infrastructure. Harassment can result from the language of correspondence, or the frequency or size of messages. A single unwelcome message can be considered harassment. Additional messages sent to an unwilling recipient, after being requested to stop by that recipient, can also be construed as harassment.

5. Defamatory or Abusive Language by using our network as a means to distribute, transmit, facilitate or post defamatory, harassing, abusive or threatening language or anything that a reasonable person would regard as hate speech or literature. This includes language or other activity that significantly prejudices, creates a hostile bias, or grossly defames a class of individuals. This policy includes links placed in websites to other materials and sites containing this type of information. Six Feet Up will be the sole arbiter in determining violations of this provision and reserves the right to take immediate action up to and including disabling your account upon receiving notice that your account contains this information.
6. Facilitating a Violation of the AUP by advertising, transmitting, or otherwise making available any software, program, product, service or information that is designed to violate, or assist in the violation of this AUP. This includes the facilitation of the means to spam, initiation of pinging, flooding, mail bombing, denial of service attacks, piracy of software, or other means or mechanisms that interrupt another's use of the Internet or another's property.
7. Illegal or Unauthorized Access to Other Computers or Computer Networks by accessing, attempting to access, monitoring, or disrupting another's account, computer, computer network, or otherwise attempting to circumnavigate the security measures of another individual's system without their permission. This type of activity is extremely harmful and could result in a severe security breach. Any activity that might be used as a precursor to an attempted system penetration is also regarded in the same manner (for example: port scan, stealth scan, or other information gathering or monitoring activity). This also includes, but is not limited to, an attempt to circumvent security in order to obtain access to services on Company servers that are not provided in your account and scanning our network or other networks with the intent to breach and or evaluate security vulnerabilities.
8. Unauthorized Reselling or Providing Access to Account Services such as offering email services and accompanying features for use by individuals outside of the required use on your own account; the reselling of CGI scripts installed on the Companies servers; or providing access codes to individuals not authorized to receive such materials as necessary for the running of your website or account.
9. Excessive CPU, Bandwidth or Disk Space Usage has the ability to compromise our shared hosting environment. This is the result of using the system in a manner that encumbers disk space, processors or other system resources beyond the allowances of your specific plan type and to the degree that your usage compromises the hosting accounts of our other customers.
10. Distribution of Internet Viruses, Worms, Trojan Horses, Denial of Service Attacks, or Other Destructive Activities by sending or distributing malicious code, or information regarding the creation of Internet viruses, worms, Trojan Horses, mail bombing or denial of service attacks, whether you actually intended to send or distribute such malicious code or information. This includes sending packets with an illegal packet size, UDP flooding, ping-flooding, half-open TCP connection flooding and any other activity that may be deemed harmful and that may result in a denial of service against any computer or computer network. Also, activities that disrupt the use of, or interfere with the ability of, others to use a computer network and any connected network, system, service or equipment. These types of activities are not only harmful to the shared hosting environment but also slow and cause damage to the entire Internet.

Intellectual Property Violations by engagement in any activity that infringes or misappropriates the intellectual property rights of others, including but not limited to copyrights, trademarks, service marks, trade secrets, software and patents held by other individuals, corporations or other entities. Our Company is required by law to respond immediately to a copyright infringement and block access to customer content upon receipt of an official notice of a copyright violation. For more information on the Digital Millennium Copyright Act (DMCA), click on the following link: <http://lcweb.loc.gov/copyright/legislation/dmca.pdf>. Common instances leading to intellectual property violations involve the unauthorized use of pictures, framing another's website within your own without permission and using another's trademarks without their permission to promote competing goods or services.

## Copyright

The Digital Millennium Copyright Act (DMCA) Procedures When we receive proper notice that your website

infringes the copyrights of another, we have a legal obligation, per Title 17 United States Code, Section 512, to "respond expeditiously to take the material down or block access to it." The procedure we follow, given our reading the DMCA [Title 17 United States Code, Section 512(c)(3)], is as follows:

1. If we receive "proper notification" of an infringing website, we send an email notice to both our customer and the individual or organization issuing the "proper notification" (hereinafter "Complaining Party"), then we deactivate the website "expeditiously." (See below regarding what "deactivate" means and note that neither the courts nor the DMCA have specifically defined what "expeditiously" means).
2. If we receive "notification," but it is not proper (i.e. more than technical errors contained within the notice), we will use our best judgment to ascertain whether the website does indeed infringe on the copyrights asserted in the notification. If we deem the website to infringe, we follow the activities in Step 1 above. If we cannot validate infringing activity, we will not "deactivate" the website, but instead send an email notice to both Customer and the Complaining Party with a statement that we opted to not "deactivate" the website because notice was not proper, and we could not determine copyright infringement; and we then request either "proper notification" or a court order.
3. If we do "deactivate" your website because of "proper notification" (not court order), our customers have two options: (a) refute the claim, or (b) remove the alleged infringing material.
  - Refuting the Claim. You may submit a "proper counter notification" (see below) to us indicating that "the material was removed or disabled through mistake or misidentification." We MUST reactive your website when we receive such a proper counter notification, in not less than 10 business days and not more than 14 business days. When we receive proper counter notification from you, we do not validate your notice or any claims, although we are required by the DMCA to forward your counter notification to the Complaining Party.
  - Removing the Alleged Infringing Material. You have the option of removing the infringing material and petitioning us to reactivate your account. To do so, you must submit an affidavit with us, specifically indicating that "under penalty of perjury that you have a good faith belief that all material alleged to infringe was removed or disabled from your website." This affidavit must contain all the components indicated in "proper counter notification," except item #3 (see below). When we receive this affidavit, we will review and forward to the Complaining Party. We may, or may not, reactivate the website at this time; although we will act as a conduit of communications between you and the Complaining Party until a resolution is achieved. Alternatively, you have the option submitting a "proper counter notification" (see "Refuting the Claim" above) once you feel your website does not contain infringing material.
4. When you file a "proper counter notification" with us, the Complaining Party has the option of obtaining a court order to prevent activation of your website. If this happens, we will comply with the court order and notify you.
5. Proper Notice of Copyright Infringement: [Title 17 United States Code, Section 512(c)(3)(A)]. For "proper notice," we require (1) a physical or electronic signature of copyright holder or authorization to act on behalf the copyright holder; (2) Identification of the copyright work alleged to be infringed on the website; (3) Identification of the material that is infringing or the subject of infringing activity; (4) Information necessary for us to contact the Complaining Party; (5) A statement that the Complaining Party has a good-faith belief that material alleged to be infringing is not authorized by the copyright holder; and (6) A statement that "the information in the notification is accurate and under penalty of perjury, that the Complaining Party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed."
6. Proper Counter Notification: [Title 17 United States Code, Section 512(g)(3)]. For "proper counter notification," we require (1) Your physical or electronic signature; (2) Identification of the material which has been removed, disabled or deactivated; (3) A statement "under penalty of perjury that you have a good faith belief that the material was removed or disabled as a result of mistake or misidentification of the material to be removed or disabled;" and (4) Your name, address, telephone number and a statement that you "consent to the jurisdiction of Federal District Court for the judicial district in which your address is located, or if your address is outside of the United States, for the United States District Court, District of New Mexico and that you will accept service of process from the person who provided notification under subsection (c)(1)(C) or an agent of such person."
7. Deactivation: Deactivation does not necessarily mean deletion. Unless under court order, or if we judge your website content to contain prohibited content, we will not delete your website content when deactivated as a result of our receiving "proper notification" of copyright infringement. Your website

content will remain on our servers for as long as your account remains in good standing with us.

8. Repeat DMCA Violations: It is our policy to terminate the privileges of customers who commit repeat violations of copyright laws.

Send notices of copyright infringements to:

ifPeople  
130 Boulevard NE, #6  
Atlanta, GA 30312 USA

## **Trademark**

Trademark Infringement is any use of a trademark, service mark, trade dress or other identifying mark, word, phrase, color, picture or layout that could lead to a likelihood of confusion between you and the legitimate holder of a valid trade or service mark. For the purposes of this AUP, a "valid trade or service mark" is defined as another entity that either has a registered mark in a WTO signatory country ([http://www.wto.org/english/thewto\\_e/whatis\\_e/tif\\_e/org6\\_e.htm](http://www.wto.org/english/thewto_e/whatis_e/tif_e/org6_e.htm)), or can prove prior use. There are relatively few "safe harbor" provisions or exceptions in United States Trademark law that limit our liability to a Customer's infringing activity of a trademark. Therefore, we take notices of alleged trademark infringement seriously, and with few exceptions, will require Customers to quickly comply. There are fair use exceptions to trademark protections. We will allow Customer to use another's trademark in fair use situations, but we apply a rather restrictive view on the meaning of fair use. If there is any possibility of a likelihood of confusion as to the originator of the offerings (product, service or information) on your website, we will side with the complaining party.

## **Alleged Trademark Infringement Procedure:**

When our Company receives notice of alleged trademark infringement activity, we will act as follows:

1. Submit a notice to the Customer.
2. If we believe there is any merit to the notice, we will give the Customer a predetermined amount of time (usually 48 hours) to take corrective action or provide unequivocal proof of either (a) permission to use trademark, or (b) that the Customer's use of trademark is superior to complaining party.
3. If the Customer fails to take corrective action, or fails to respond with unequivocal proof as required above, we will deactivate the account.

Obscene Speech or Materials by using our computer network to advertise, transmit, store, post, display or otherwise make available child pornography or obscene speech or material. All material on our network and servers must comply with United States laws. Furthermore, all material placed on our network and servers by our customers must be legal in their own jurisdiction. For child pornography, we immediately notify law enforcement agencies when we become aware of the presence of child pornography on or being transmitted through our network.

Defamatory or Abusive Language by using our network as a means to distribute, transmit, or post defamatory, harassing, abusive or threatening language or anything that can be regarded as hate literature. This policy applies to anything that is not protected under free speech.

Other Illegal Activities where the transmission or storage of any information, data or material is in violation of United States Federal or State regulations. Engaging in activities that are determined to be illegal, including advertising, transmitting or otherwise making available ponzi schemes, pyramid schemes, fraudulently charging or collecting credit cards or information and pirating software. Activities may be deemed illegal according to the laws and jurisdictions of where the activity is generated, as well as according to the jurisdiction of where the activity is directed.

Other Activities or Information, lawful or unlawful, that we deem harmful, offensive, controversial, infamous or other to either the Company, its customers, or third-parties, such that we reasonably believe our customers, operations, reputation, goodwill or general customer relations could potentially be negatively impacted.  
Remedies and Action

Responsibility of avoiding the above harmful activities rests solely on you, our Customer. We do not, and will

not, monitor website content or communications of our customers. However, if we learn of a violation of our AUP, we will respond accordingly and at our sole discretion. The type of action taken will depend on the severity and duration of the violation, as well as perceived breadth and severity of the harm to us, or others. When we become aware of an alleged violation of our AUP, we will (as quickly as practical) investigate the claim and determine the course of action necessary to remedy the problem. No credits will be issued for down time incurred if the account is suspended (i.e. "deactivated") or deleted due to what we perceive as a violation of this AUP, whether or not it is later proven that any AUP violation existed.

One or more of the following responses may occur:

- A warning is issued to the account holder.
- A request is issued to remove offending content.
- The hosting account is suspended (i.e. "deactivated").
- A monetary deposit is requested as assurance against future behavior (i.e. "security deposit").
- The hosting account is deleted, such that all information is permanently and irretrievably removed from our servers, potentially without your knowledge or notice.
- Action is taken in accordance with our AUP, Service Agreement, or applicable law.
- In certain egregious circumstances, we may notify the proper legal authorities.

## **Customer Security Responsibilities**

The Customer is solely responsible for any breaches that occur in servers, equipment, services or daemons under client's control. If a client's account is exploited and used for any violation of our AUP or used for destructive or disruptive purposes of any kind, it will be shut down immediately for investigation and cleaning. Any labor needed to fix such a breach and/or any damage done is currently charged at \$99 USD per hour to the offending client.

## **Miscellaneous**

**Monitoring** - We will not intentionally monitor private email messages sent or received by our customers, unless required to do so by law or court order. However, we reserve the right to monitor our servers and equipment, which may include your data and information, to ensure that our systems are operating optimally.

**Disclosure of Private Information** - We will not disclose private customer information unless compelled by law or court order.

**Practicality / Timeliness** - We will react to notices regarding violations as quickly as practical, given our judgment as to the potential harm and consequences of the alleged violation.

**Proof** - In instances where alleged AUP violations by our customers have not been substantiated by the notice sent to our Company and the accuracy of the notice cannot be substantiated by us after a review of the facts, we reserve the right to use our best judgment on who bears the burden of proof for or against the alleged AUP violation. In such cases, we generally place the burden of proving the AUP violation on the complaining party. However, there are some instances where we may place the burden of proving an AUP violation did not occur on our customer - these instances will usually involve what we view as a protected class (i.e. potential harm to minors).

**Jurisdiction** - We always apply the laws of the United States and the State of Indiana to any legal analysis by our Company. We will also apply, when and where applicable for a particular website, the laws of the jurisdiction where our Customer sits, the jurisdiction(s) directly targeted or marketed (through proactive means) by our Customer and the jurisdiction that "owns" content on our customer's website (i.e. Australian law will be used for subject matter containing photos of an Australian movie star).

We hope that this AUP is helpful in clarifying the obligations of our customers and their subscribers, as responsible users of the Internet.

Please see [www.ifpeople.net/policies](http://www.ifpeople.net/policies) for all ifPeople policies and most recent versions.