



Webjogger Acceptable Use Policy (“AUP”)

The Service may only be used for lawful purposes. Transmission, retransmission, distribution, or storage of any information, data, communication, material or content (hereinafter known as "Content") in violation of any federal or state law or regulation is strictly prohibited. The aforementioned shall include, but is not limited to, copyrighted Content, Content which infringes any trademark, trade secret, or other intellectual property right, violates export control laws or regulations, or violates any party's confidentiality rights; Content which is used to alter, steal, corrupt, disable, destroy, trespass or violate any security or encryption computer file, database or network; threats, harassment, obscene or indecent, pornographic (including child pornography -- Webjogger is required by law to notify law enforcement agencies when it becomes aware of the presence of child pornography on or being transmitted through Webjogger's network), defamatory, libelous, threatening, abusive, hateful or excessively violent Content, or Content that would encourage any action that would constitute a criminal offense whether defined by local, state, federal or international law.

Customer agrees to indemnify and hold harmless Webjogger, its parent company, any affiliated companies, each of their respective officers, directors, employees, shareholders, and agents (herein “Indemnified Party” or “Indemnified Parties”) from any and all claims, damages, losses, liabilities, suits, actions, demands, proceedings (whether legal or administrative) and expenses (including but not limited to reasonable attorney's fees), asserted, filed by a third party against any of the Indemnified Parties to the extent caused by Customer's unlawful use of this Service, Customer's violation of the Acceptable Use Policy, any breach by Customer of any material terms or conditions of this Agreement and its representations and warranties hereunder, or any unlawful or negligent acts of omissions of Customer which damages Customer, Webjogger, or a third party. The obligation to indemnify provided herein shall survive termination of this Agreement.

Customer further agrees that it shall not, nor shall it permit others to:

- alter, tamper with, adjust, repair or circumvent any aspect of the Services; or
- resell, pass-through, sublicense, rent, lease, timeshare or rebrand the Services or otherwise provide the Services to any party not within Customer's enterprise and related personnel.

Customer will be held responsible for the action of any third party agent that acts on behalf of, or for the benefit of, Customer and with Customer's knowledge and consent. Customer shall be held directly accountable for any violations of this Acceptable Use Policy by such third party agents.

Webjogger does not control the content of data traversing Webjogger networks; accordingly, Webjogger assumes no responsibility for the content of any data or communication that may be transmitted over Webjogger networks.

Prohibited Uses

These lists are not meant to be exhaustive, but merely illustrative of examples of inappropriate and improper conduct which is prohibited on Webjogger networks.

Abuse

The following general actions are considered "abuse" and are strictly prohibited:

- Any conduct which is inconsistent with generally accepted norms and expectations of the Internet community (whether or not detailed in this AUP). Webjogger reserves the right, in its sole discretion, to make a determination whether any particular conduct violates such norms and expectations.



- Forging message headers or identity information, or taking any action with the intent of bypassing restrictions or limits on access to a specific service or site. This prohibition does not restrict the legitimate non-commercial use of pseudonymous or anonymous services.
- Falsifying identity or contact information (whether given to Webjogger, a Registrar, or other parties).
- Sending or distributing information regarding the creation of any virus, worm, Trojan horse or harmful code or attachment.
- Knowingly engaging in any activities designed to harass, or that will cause a denial-of-service (e.g., synchronized number sequence attacks) to any other user whether on the Webjogger network or on another provider's network.
- Violating the acceptable use policies of Webjogger's upstream Internet providers.
- Advertising, transmitting, or otherwise making available any software, program, product, or service that is designed to violate this Acceptable Use Policy, which includes the facilitation of the means to SPAM, initiation of pingging, flooding, mail bombing, denial of service attacks, and piracy of software.

Security

Users of Webjogger networks must configure their systems in a secure manner. Should unauthorized persons exploit Customer's system, Customer is responsible for both reporting the violation (where applicable), and then fixing the exploited system. For instance, should the security of a mail server be compromised to distribute unsolicited emails, Customer is responsible for immediately re-configuring the system to prevent further unauthorized use.

Customer is prohibited from

- Interfering or attempting to interfere with services ("Denial of Service Attacks"), whether intentionally or through neglect, of any other user, host, or network. The prevention of "unintentional attacks", such as infection and subsequent propagation of computer viruses, are the responsibility of every Customer: anti-virus software should be installed on every system which connects to Webjogger networks.
- Accessing illegally or without authorization computers, accounts, or networks belonging to another party, or attempting to penetrate security measures of another individual's system (often known as "hacking"). This prohibition extends to any activity that might be used as a precursor to an attempted system penetration (i.e. port scan, stealth scan, or other information gathering activity).
- Injecting, intentionally or negligently, false or unauthorized network control data into Webjogger networks, for instance in the form of incorrect routing or DNS information.

E-Mail

Customer is prohibited from engaging in improper use or distribution of electronic mail ("e-mail"). Customer is strictly prohibited from engaging in any of the following activities:

- Sending unsolicited mass or commercial e-mail ("spamming") for any purpose whatsoever.
- Having third parties send out unsolicited commercial emails on Customer's behalf.
- Using Webjogger facilities to receive replies from unsolicited emails (commonly referred to as "drop-box" accounts).
- Configuring any email server in such a way that it will accept third party emails for forwarding (commonly known as an "open mail relay"). If a site has roaming users who wish to use a common mail server, the mail server must be configured to require some form of user identification and authorization.
- Running unconfirmed mailing lists. Subscribing email addresses to any mailing list without the express and verifiable permission of the email address owner is prohibited. All mailing lists run by Webjogger Customers must be Closed-loop ("Confirmed Opt-in"). The subscription confirmation message received from each address owner must be kept on file for the duration of the existence of the mailing list. Purchasing lists of email addresses from 3rd parties for mailing to or from any Webjogger network is prohibited.



Mass or commercial email may be sent only to recipients who have expressly requested receipt of such e-mails, by the sending of an email request to the person performing the mass or commercial mailings. This exchanging of requests, acknowledgements, and final confirmations (commonly referred to as a "double opt-in" process) must be adhered to in their entirety for any mass or commercial email to be considered "solicited" by Webjogger.

Customers that send mass or commercial e-mail are required to maintain complete and accurate records of all e-mail subscription requests, specifically including the email and associated headers sent by every subscriber, and to immediately provide Webjogger with such records upon request of Webjogger. Subscriptions that do not have a specific recipient-generated email request associated with them are invalid, and are strictly prohibited.

In the absence of positive, verifiable proof to the contrary, Webjogger considers complaints by recipients of e-mails to be de-facto proof that the recipient did not subscribe or otherwise request the e-mail(s) about which a complaint was generated.

Usenet (also known as Netnews or Newsgroups)

Webjogger recommends that Customer does not post to any newsgroup until Customer they have familiarized themselves with the subjects, established guidelines, and restrictions of such newsgroups. All Usenet guidelines and restrictions are incorporated herein by reference, and users of Webjogger networks agree to adhere to such guidelines unconditionally.

Without limitation of the foregoing, it is strictly prohibited to engage in any of the following activities:

- Making any posting for commercial purposes (including without limitation the pointing to specific URLs for commercial purposes), except where such postings are expressly permitted under the charter and/or Frequently Asked Questions (FAQ) of an applicable newsgroup.
- Posting binary files to newsgroups whose charter or name does not include allowances for such files.
- Canceling newsgroup postings other than your own, or using auto-responders or cancel-bots (except in cases of official newsgroup moderators performing their duties).
 - "Excessive Cross-Posting" (ECP) or "Excessive Multi-Posting" (EMP), or "Usenet spam": Webjogger retains the exclusive right to define these and other terms, however, we generally defer to the definitions found at <http://www.cybernothing.org/faqs/net-abuse-faq.html>
 - Disrupting newsgroups with materials, postings, or activities that are (as determined by Webjogger in its sole discretion), excessive, or repetitious, unless such materials or activities are expressly allowed or encouraged under the newsgroup's name, FAQ, or charter.
 - Performing any unauthorized creation, cancellation, or removal of newsgroups.

The legitimacy of a given post or cancellation is generally determined by the official newsgroup or mailing-list moderator, therefore, Webjogger usually defers to their judgment on these issues, however, Webjogger retains the exclusive right to make these determinations.