

## Acceptable Use Policy

Weblosoft's Acceptable Use Policy ("AUP") is provided to give our customers and users a clear understanding of what we expect of them while using the service. All users of our services: those who access some of our Services but do not have accounts, as well as those who pay a service fee to subscribe to the Services, must comply with this AUP and our Terms of Service. Usage of Weblosoft's services constitute acceptance and agreement to our AUP as well as our Terms of Service. This Acceptable Use Policy applies to all persons and entities (collectively, "customers") using the products and services of Weblosoft ("the company") including Internet service. The policy is designed to protect the security, integrity, reliability, and privacy of both the company's network and the products and services Weblosoft offers to its customers. Weblosoft reserves the right to modify this policy at any time, effective immediately upon posting of the modification. Your use of Weblosoft's products and services constitute your acceptance of the Acceptable Use Policy in effect at the time of your use. You are solely responsible for any and all acts and omissions that occur during or relating to your use of the service, and you agree not to engage in any unacceptable use of the service. Due to the myriad of possibilities in maintaining a network, this document is intended to act as a guideline to service and not to be all encompassing. Legal action may be taken by Weblosoft or the appropriate police force in certain circumstances. We support the uncensored flow of information and ideas over the Internet and do not actively monitor subscriber activity under normal circumstances. Similarly, we do not exercise editorial control over the content of any website, e-mail transmission, newsgroups, or other material created or accessible over or through the services, except for certain proprietary Web sites. However, in accordance with our TOS (Terms of Service), we may remove any materials that, in our sole discretion, may be illegal, may subject us to liability, or which may violate this AUP. Weblosoft may cooperate with legal authorities and/or third parties in the investigation of any suspected or alleged crime or civil wrongdoing. Your violation of this AUP may result in the suspension or immediate termination of either your Easy Internet Solutions account or other actions WITHOUT PRIOR NOTICE. We do not routinely monitor the activity of accounts except for measurements of system utilization, the preparation of billing records and during technical support requests. However, in our efforts to promote good citizenship within the Internet community, we will respond appropriately if we become aware of inappropriate use of our service. You may not use your account to publish material, which Easy Internet Solutions determines, at its sole discretion, to be unlawful, indecent or objectionable. For purposes of this policy, "material" refers to all forms of communications including narrative descriptions, graphics (including photographs, illustrations, images, drawings, logos), executable programs, video recordings, and audio recordings.

### Direct violation examples

Direct violations of our Acceptable Use Policy include, but is not limited to, any of the following:

#### **Copyright infringement. Including, but not limited to:**

- Installation/distributed of “pirated” or other software products that are not appropriately licensed for use by you.
- The hosting of “screeners”, “pirated” DVDs or other movie or audio files that you do not have written permission from the copyright holder to reproduce on the internet
- Transmission or storage of material that infringes any copyright, trademark, patent, trade secret or other proprietary rights of any third party

**Spam. Including, but not limited to:**

- The sending or receiving of mass unsolicited email (SPAM) is a direct violation of the acceptable use policy. This includes the direct sending and receiving of such messages, support of such messages via a web page, splash page or other related sites, or the advertisement of such services.
- The sending, return, bouncing or forwarding of email to specified user(s) in an attempt to interfere with or over flow email services is a direct violation of the acceptable use policy.
- The use of the services to proxy email unsolicited users is a direct violation of the acceptable use policy. Proxy email is defined as the use of dedicated services to act in concert with other services located inside and outside the network to achieve mass unsolicited email (SPAM) to unrelated third parties
- The use of dedicated services to send, receive, forward, or post-UseNet unsolicited email or posts is a direct violation of the acceptable use policy.

**Illegal use. Including, but not limited to:**

- Sending or promotion of: death threats, terroristic threats, threats of harm to another individual, multi-level marketing schemes, “Ponzi schemes”, invasion of privacy, credit card fraud, racketeering, defamation, slander, and other common illegal activities.
- Creating or forwarding “chain letters” or other “pyramid schemes” of any type.
- Hosting, sending or promotion of: Child pornography, bestiality or necrophilia
- Threats or harassment to individuals, organizations or businesses
- Sending or promotion fraudulent activities
- Hosting, send or promotion of sites advocating human violence and hate crimes based on religion, ethnicity, or country of origin
- Any activity associated with Phishing or systems designed to collect personal information (name, account numbers, usernames, passwords, etc.) under false pretence.
- Harassment, whether through language, frequency, or size of messages.
- Unauthorized use or forging of mail header information.
- Exporting, re-exporting, or permitting downloads of any content in violation of the export or import laws of the United Kingdom or without all required approvals, licenses and exemptions.
- Any material which is in breach of the criminal law, including material judged to be obscene under the current interpretation of the Obscene Publications Act 1959.
- Material likely to encourage an interest in sexually abusive activity (eg paedophilia, incest, rape) which may include adults role-playing as non-adults.

- The portrayal of any sexual activity which involves a lack of consent (whether real or simulated). Any form of physical restraint which prevents participants from indicating a withdrawal of consent.

**Denial of service. Including, but not limited to:**

- Origination or control of denial of service attacks or distributed denial of service attacks
- Any actions that restrict or inhibit anyone – whether a customer of Weblosoft or otherwise – in his or her use or usage of our products and services or that generate excessive network traffic through the use of automated or manual routines that are not related to ordinary personal or business use of Internet services.

**Malware. Including, but not limited to:**

- Storage, distribution, fabrication, or use of malware including virus software, rootkits, password crackers, adware, key stroke capture programs and other programs normally used in malicious activity. Programs used in the normal ordinary course of business are deemed acceptable.
- Introduction of malicious programs into our network or servers or other products and services of Weblosoft (e.g., viruses, Trojan horses and worms)
- Executing any form of network monitoring that will intercept data not intended for the customer.

**Security breaches. Including, but not limited to:**

- Circumventing user authentication or security of any host, network or account.
- Causing or attempting to cause security breaches or disruptions of Internet communications. Examples of security breaches include but are not limited to accessing data of which you are not an intended recipient, or logging into a server or account that you are not expressly authorized to access. Examples of disruptions include but are not limited to port scans, flood pings, packet spoofing and forged routing information.
- Furnishing false or incorrect data on the order form contract (electronic or paper) including fraudulent use of credit card numbers or attempting to circumvent or alter the processes or procedures to measure time, bandwidth utilization or other methods to document usage of the products or services.

**IRC networks. Including, but not limited to:**

- It is absolutely forbidden to host an IRC server that is part of or connected to another IRC network or server

**Running of software that listens on any TCP/UDP port. Including, but not limited to:**

- BitTorrent trackers

**Forwarding of emails to AOL or Hotmail email addresses:**

- It is prohibited to forward emails from your cPanel control panel to address operated by AOL (such as those ending aol.com and aol.co.uk) or Hotmail (such as hotmail.com or hotmail.co.uk). This is due to their anti-spam policies which may result in our servers being blocked if a spammer sends you a spam email which then gets automatically forwarded to these providers.

## **Fair usage**

Weblosoft accounts operate on shared resources. Excessive use or abuse of these shared networks and hosting resources by one customer may have a negative impact on all other customers. Misuse of network resources in a manner which impairs network or server performance is prohibited by this policy and may result in termination of your account.

- You are prohibited from excessive consumption of resources, including CPU time, memory, disk space and session time. You may not use resource-intensive programs which negatively impact other customers or the performances of Weblosoft systems or networks. Weblosoft reserves the right to terminate or limit such activities.
- Any account using more than 30 minutes of CPU time per day is deemed to be exceeding our shared resources. CPU time levels can be viewed in the Client Area.
- Any scheduled tasks – run via cron or any other method – must run with an interval no smaller than once every 5 minutes and must run for no more than 20 seconds.
- MySQL queries must not run for more than 20 seconds – queries exceeding that limit may be killed. Table indexes must be sufficient to prevent slow joins.
- Files & directories on an account (inodes) have variable limits which vary per package. These limits are viewable from within cPanel.
- All accounts have email sending limits, which varies per package. This doesn't affect inbound emails. Any emails sent beyond the limit will be rejected.
- Any website receiving an abnormally high level of hits per second (including both dynamic and static content) may be temporarily suspended if the load is found to affect other users of the server.

Scripts are known to cause a high level of resource usage, or those that automatically refresh themselves, are forbidden. Examples include, but aren't limited to:

- Anything IRC related
- Proxy or anonymising systems
- Spiders/crawlers/indexers
- Scripts automatically refreshing more frequently than once every 60 seconds

## **CPU / RAM / IO Limits**

Our cPanel shared hosting packages come with limits on CPU, RAM and IO usage.

The limits are available to view from inside your cPanel account, it's possible to upgrade these limits by moving to a higher plan.

### **Automated email**

You are permitted to configure items such as IP cameras, alarms and other IoT devices with email accounts which are provided by us as part of your hosting account, on the condition that the device will only send a reasonable amount of mail. For example, a device that sends an email every second whilst triggered/active is not allowed and will result in the associated mailbox being disabled. You must configure such devices properly to prevent this.

### **Unlimited Bandwidth**

Some of our shared hosting packages offer unlimited bandwidth. The intention of providing unlimited bandwidth is to eliminate the need to worry about bandwidth use. While there is no explicit limit, we do have to ensure individual websites do not cause excessive usage that upsets or interrupts other users of the shared servers. All packages offering unlimited bandwidth are intended for personal or small business websites.

In addition to bandwidth, there are other finite server resources such as CPU and memory; all accounts making use of unlimited bandwidth must still abide by the resource limits as described by the Fair Usage section.

Accounts taking advantage of unlimited bandwidth must not:

- provide audio/video files for download
- use the account as a "file dump" for files unrelated to the website
- monopolise bandwidth or destabilise the service through excessive usage
- Accounts found to be causing instability, consuming excessive resources, or otherwise exceeding these restrictions may have a fixed bandwidth limit imposed at our sole discretion. We endeavour to contact the account owner prior to taking corrective action in all cases where server stability isn't being compromised. As resources are shared with other users if one account is causing instability, we may need to temporarily suspend it until the excessive usage stops.

### **Unlimited Web Space**

Some of our shared hosting packages offer unlimited web space. The intention of providing unlimited web space is to eliminate the need to worry about your disk usage. While there is no explicit limit, we do have to ensure individual accounts do not cause excessive usage that interrupts other users of the shared servers. All packages offering unlimited web space are intended for personal or small business websites.

Server hard disks are finite in size; while we will scale with the capacity it is expected that individual accounts be respectful of other users sharing the server and not exceed many multiples of the average disk usage.

Accounts taking advantage of unlimited web space must not:

- Use the account as a “file dump” for files unrelated to the website.
- Use the account as a backup for any computers or other devices, or backups of the live website.
- Store very large amounts of email. Individual email accounts storing over 1GB of email may be required to reduce their usage to under 1GB if requested by technical staff.
- Monopolise other finite resources such as CPU or memory.
- Accounts found to be causing instability, consuming excessive resources, or otherwise exceeding these restrictions may have a fixed web space limit imposed at our sole discretion. We endeavour to contact the account owner prior to taking corrective action in all cases where server stability isn't being compromised. As resources are shared with other users if one account is causing instability, we may need to temporarily suspend it until the excessive usage stops.
- Store multiple backups of site content within the account, including but not limited to, cPanel backups, automated Softaculous backups.

All our packages contain limits on the number of files that can be stored in the hosting account, but not the size of the files themselves.

Files may be removed without notice from hosting accounts where this is deemed to have taken place.

### **Unlimited Add-on Domains**

Some of our shared hosting packages offer unlimited add-on domains. The intention of providing unlimited add-on domains is to eliminate the need to worry about the number of websites you host. While there is no explicit limit, we do have to ensure individual accounts do not cause excessive usage that interrupts other users of the shared servers. All packages offering unlimited add-on domains are intended for personal or small business websites.

For the avoidance of doubt normal usage of add-on domains to host websites is acceptable; the abusive adding of hundreds or thousands of add-on domains is not acceptable.

### **Abusable Resources**

Upon notification of the existence of an abusable resource (for example, an insecure form mail script, outdated software installation or smurf amplifier), the customer shall immediately take all necessary steps to avoid any further abuse of such resource. Any abuse of an open resource that occurs after the customer has received such notification shall be considered a violation of this policy and enforced as such.

### **Use of finite resources**

Easy Internet Solutions reserve the right to restrict access to finite resources such as, but not limited to, CPU, RAM, disk access, where customer applications, scripts or other static or dynamic applications consistently consume above average use.

### **Providing services to others**

You must not:

- resell or give away any of our free-of-charge hosting services to any person
- use any of our free-of-charge hosting services to provide a hosting service (whether paid-for or free) to any person (excluding the inclusion of a third party's advertisements on your website).

### **Enforcement**

Weblosoft may immediately suspend and/or terminate the customer's service for violation of any provision of this policy upon verbal or written notice, which notice may be provided by voicemail or E-mail. Prior to suspension or termination, Weblosoft attempts to work with our customers to cure violations of this policy and ensure that there is no re-occurrence; however, Weblosoft reserves the right to suspend or terminate based on a first offence.

No failure or delay in exercising or enforcing this policy shall constitute a waiver of the policy or of any other right or remedy. If any provision of this policy is deemed unenforceable due to law or change in the law, such a provision shall be disregarded, and the balance of the policy shall remain in effect.

### **Security**

You are responsible for any misuse of your account, even if the inappropriate activity was committed by a friend, family member, guest or employee. Therefore, you must take steps to ensure that others do not gain unauthorized access to your account. In addition, you may not use your account to breach the security of another account or attempt to gain unauthorized access to another network or server.

- Your password provides access to your account. It is your responsibility to keep your password secure.
- Sharing your password and account access with unauthorized users is prohibited. You should take care to prevent others from using your account since you will be held responsible for such use
- Attempting to obtain another user's account password is strictly prohibited and may result in termination of service.
- You must adopt adequate security measures to prevent or minimize unauthorized use of your account.
- You may not attempt to circumvent user authentication or security of any host, network or account. This includes, but is not limited to, accessing data not intended for you, logging into or making use of a server or account you are not expressly authorized to access or probing the security of other networks. Use or distribution of tools designed for compromising security is prohibited.

Examples of these tools include, but are not limited to, password guessing programs, cracking tools or network probing tools.

- You may not attempt to interfere with service to any user, host or network (“denial of service attacks”). This includes, but is not limited to, “flooding” of networks, deliberate attempts to overload a service, and attempts to “crash” a host.
- Users who violate systems or network security may incur criminal or civil liability. Weblosoft will cooperate fully with investigations of violations of systems or network security at other sites, including cooperating with law enforcement authorities in the investigation of suspected criminal violations.
- Weblosoft customers will be held responsible and accountable for any activity by third parties, using their account, that violates guidelines created within the Acceptable Use Policy.

### **Account Security**

Some of our packages may come with or offer as an add-on, software update notification and vulnerability scanning services. These include, but are not limited to, Fantastico software updates, cPanel add-on updates and Malwise.

These services offer scanning and notification only, without the guarantee that all vulnerabilities have been detected. Malicious code can be hidden in many ways and, like a virus scanner on your computer, we can only detect malicious code that is known to be bad and, to a lesser degree, unknown code that we believe may be bad.

Should an account be found to contain malicious code, a separate service may be required to affect its removal if you are unable to do so yourself. Similar to vulnerability scanning, such removal does not come with a guarantee that all malicious code has been removed.

### **Electronic Communications Privacy Act Notice**

Weblosoft makes no guarantee of confidentiality or privacy of any information transmitted through or stored upon Weblosoft technology and makes no guarantee that any other entity or group of users will be included or excluded from Weblosoft’s network. In addition, Weblosoft may periodically monitor transmissions over its network for maintenance, service quality assurance or any other purpose permitted by the Electronic Communications Privacy Act.

We retain the right, at our sole discretion, to refuse new service to any individual, group, or business. We also retain the right to discontinue service with notice for repeated violation of the acceptable use policy over time.