

Acceptable Use Policy

www.dlrmedia.co.uk

Acceptable Use Policy

This is the Acceptable Use Policy ("**Policy**") for DLR Media Limited ("**we/us**").

This Policy is necessary to ensure that we may continue to provide the best possible service to all of our customers whilst at the same time satisfying our legal and ethical responsibilities.

Failure to follow any condition of the Policy will be grounds for immediate suspension of our services without notice. We will be the sole arbiter as to what constitutes a violation of any of these provisions. If we suspend our services the customer will not be entitled to repayment of any fees.

To report suspected abuses or any violations of this Policy, please contact us by email.

- 1) **Illegal Usage.** Our servers may be used for lawful purposes only. Transmission, storage, or distribution of any information, data or material in violation of any applicable law or regulation is prohibited. This includes, but is not limited to: copyrighted material, trademark, trade secret or other intellectual property right used without proper authorisation, and material that is obscene, defamatory, constitutes an illegal threat, or violates export control laws. Any forum/discussion board discussing where to obtain such files or a forum/discussion that distributes such files is prohibited. Customers agree to indemnify us and hold us harmless from any claims resulting from the use of our hosting service. We will be the sole arbiter as to what constitutes a violation of this provision.
- 2) **Illegal Content.** Our hosting service does not allow customers to use any background daemons (for example IRC bots, eggdrop, BitchX or XiRCON) or any other program that interferes with normal server operation. The customer is not permitted to use warez or web proxies, including NPH-Proxy. If a customer's site is found to hold any proxy files, their account will be suspended. When a customer is using an account with shell, they are not allowed to run any of the following servers or services on our hosting network: perlbots, proxies, BitchX, psyBnc, root exploits, DDoS scripts, Shoutcast servers, and any similar services. If a customer runs any of the aforementioned servers or services we will immediately suspend the customer's account and reserve the right to terminate that account, at our sole discretion.
- 3) **Software Distribution.** Our web hosting accounts may not be used for the purposes of distributing software and multimedia products, unless otherwise agreed in writing with us.
- 4) **File Usage & Storage.** Our web hosting accounts may not be used to distribute files in excess of reasonable server resources. Customers may use their storage space for personal use.
- 5) **Chat Rooms.** Our hosting service does not allow chat rooms on shared hosting environments. Please note that chat rooms are distinct from and should not be confused with a live chat service.
- 6) **IRC.** Our hosting service does not allow IRC or IRC bots to be operated on shared or reseller servers. IRC or IRC bots are allowed on dedicated servers provided that there are no negative impacts on our network.
- 7) **Security.** Users are prohibited from violating or attempting to violate the security of our hosting service. If this occurs, we will conduct an investigation, which may involve cooperation with police authorities. These violations of our security include, without limitation:

- a) Accessing data not intended for user or logging into a server or account, which such user is not authorised to access;
- b) Attempting to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without proper authorisation;
- c) Attempting to interfere with service to any user, host or network, including, without limitation, via means of overloading, "flooding", "mail bombing" or "crashing";
- d) Forging any TCP/IP packet header or any part of the header information in any e-mail or forum posting;
- e) Taking any action in order to obtain services to which such user is not entitled; and
- f) Attempting to couple many hosting packages together to take advantage of massive space or bandwidth allocations.

Users may add a security package from us at any time, however we are not liable for failure in respect of failure of the service or for any cyber attacks.

- 8) **Server Abuse.** Any attempts to undermine or cause harm to our server is strictly prohibited.
 - 9) **Customer Responsibility.** Customers are responsible for all activity originating from their account unless they are able to prove to our satisfaction that the activity is a result of hacking or forgery by a third party. Customers are responsible for securing their username/password. Customers are solely responsible for all third party material on their site that.
 - 10) **Backups.** We make reasonable efforts to maintain the integrity of our hosting system. However, we shall not be held responsible for loss of customer data in relation to our hosting service. We recommend that customers back up all information on their own systems. Our hosting service data backups are designed against hardware failure, and not customer user error. We do not guarantee that any backups we take will be fit for customer purposes. We cannot guarantee to customers that we can provide back ups of their data.
 - 11) **Actions Taken.** The failure by a customer to meet or follow any of this Policy is grounds for account deactivation. We will be the sole arbiter as to what constitutes a violation of the Policy. We reserve the right to remove any account without prior notice.
- When we become aware of an alleged violation of this Policy, we will initiate an investigation. During the investigation, we may restrict a customer's access to the services in order to prevent further potentially unauthorised activity. Depending on the severity of the violation, we may, at our sole discretion, restrict, suspend, or terminate a customer's web hosting account. If such violation is a criminal offence, we will notify the appropriate authorities of such violation.
- We do not issue credits for outages as a result of our disabling customer services due to their alleged violation of this Policy.
- 12) **Resource Abuse Policy.** Any customer whose website uses a high amount of our shared servers (as determined by us) resources (CPU, memory usage, and network resources) will be given an option to pay for their own dedicated server.

- 13) **Average Server Usage Limits.** Our average server usage limits are as follows:
- a) Memory usage may not exceed 10% per domain/file/application;
 - b) CPU usage may not exceed 15% per domain/file/application;
 - c) Apache connections may not exceed 30 connections;
 - d) 15 MySQL maximum user connections allowed; and
 - e) 350 emails per hour, per domain.
- 14) **Suspensions.** We may suspend our services where a customer's usage is over the service limits set out in paragraph 13. If the services are so suspended and the customer does not wish to pay for a dedicated server, we will only release the suspension within 24-48 hours. We may provide a backup of customer files or will allow the customer to access its FTP or cPanel, at our sole discretion.
- 15) **Mail Policy.** Our default allowance per domain is 60 checks per hour. Where relevant to the services we provide to the customer if we find a customer account is transmitting email to persons that did not authorise such activity, we may suspend and/or terminate the customer's website.
- 16) **Sending Unsolicited Bulk Email.** The sending of any form of Unsolicited Bulk Email ("UBE") through our or any of our third party providers' servers is prohibited. Likewise, the sending of UBE from another service provider advertising a web site, email address or utilizing any resource hosted on our or any of our third party providers' servers is prohibited. Our accounts or services may not be used to solicit customers from, or collect replies to, messages sent from another internet service provider where those messages violate our contract with the relevant customer or any terms of the other provider. Where relevant to the services we provide to the customer, the customer must not email any third parties who have not specifically asked to receive emails from the customer. If we become aware of a customer emailing third parties who have not asked to receive emails from the customer, we may suspend or terminate the services we provide to that customer.
- 17) **Running Unconfirmed Mailing Lists.** Where relevant to the services we provide to the customer, customers may not subscribe email addresses to any mailing list without the express and verifiable permission of the email address owner. All customer mailing lists in relation to the services we provide must be closed-loop. The subscription confirmation message received from each address owner must be kept on file for the duration of the existence of the mailing list. Customers may not purchase lists of email addresses from third parties in relation to the services we provide.
- 18) **Operating an account on behalf of, or in connection with, or reselling any service to, persons or firms listed in the Spamhaus Register of Known Spam Operations (ROKSO) database at www.spamhaus.org.** Where relevant to the services we provide to the customer, if we become aware of more than three complaints logged against a customer's website on Spamhaus, AOL or SpamCop or any other similar website in a 24 hour period, we may suspend our services. Services may be reinstated if the customer provides a satisfactory explanation to us for the complaints, at our sole discretion.
- 19) **Connectivity.** Hosting services and domain hosting are provided on our behalf by a third party supplier. Our suppliers endeavour to have network connectivity available for http access 99% of the time but do not guarantee this will be the case. We will have no liability if a customer's website is not accessible.