

Visicom Hosting
Acceptable Use Policy
(V2.1)

ACCEPTABLE USE POLICY

Any user of Visicom Hosting services ("Services") must comply with this Acceptable Use Policy (AUP). Visicom Hosting may change this Policy to reflect any changes in the law or community standards or whenever Visicom Hosting deems it necessary. Any changes will be effective upon posting to the email address provided by the Client and it will be the Client's responsibility to ensure that they are fully aware of these changes. For the purposes of this Policy, "you" is the Client and "we" or "us" is Visicom Hosting.

1. ILLEGAL USE

Services may be used for lawful purposes only and in compliance with all statutes in force at the time. You agree not to use Services to store, send or receive materials or data in breach of any law or regulation or which is defamatory, offensive, abusive, indecent, obscene or in breach of confidence, privacy, trade secrets or in breach of any third party intellectual property rights (including, but not limited to, copyright) or in breach of any other rights.

2. BREACHES OF SYSTEM OR NETWORK SECURITY

Any breach by you of our systems or network security or those of our licensors is prohibited, and may result in you facing criminal and civil liability. We will investigate incidents involving such breaches and will inform and co-operate with the relevant law enforcement authorities. Security breaches may include, but are not limited to, the following:

Unauthorised access to or use of our data, systems or networks or those of our licensors, including any attempt to probe, scan or test the vulnerability of a system or network;

Unauthorised monitoring of data or traffic on any of our networks or systems or those of our licensors without express authorisation of the owner of the relevant system or network; or

Interfering with any user, host or network including mailbombing, flooding, deliberate attempts to overload a system and broadcast attacks.

You may not store or distribute certain other types of prohibited material on our servers, or on servers connected to the Internet using our connectivity or that of our licensors. Examples of prohibited material include, but are not limited to, programs containing viruses or Trojan horses and tools to compromise the security of other sites, programs designed to send or encourage or facilitate the sending of unsolicited direct marketing emails, or programs or services designed to encourage or facilitate a breach of this Policy or the AUP at other sites.

3. EMAIL USE

We will investigate complaints regarding e-mail and may take action based on the rules set out below. If an e-mail message is found to violate one of the policies below, or to contain unlawful material, as described in Clause 1 above, we may take action as outlined in Clause 6 below.

You may not send e-mail to any user who does not wish to receive it, either at Visicom Hosting or elsewhere. We recognise that e-mail is an informal medium, however, you must refrain from sending further e-mail to a user after receiving a request to stop.

Unsolicited direct marketing emails via our Services, whether commercial or informational, are strictly prohibited. You may send advertising or marketing material using our Services only to addresses that have specifically requested it. We will not forward mail of accounts terminated for bulk mailing or sending unsolicited advertising material. Chain letters are unsolicited by definition and may not be propagated using our Services.

You may not send, distribute, or reply to mailbombs using our Services. Mailbombing is defined as either e-mailing copies of a single message to many users, or sending large or multiple files or messages to a single user, with malicious intent.

In using our Services, you may use aliases that are part of your Service provision but you may not use false email headers or alter the headers of email messages to conceal the email address or to prevent an Internet Client from responding to messages. You must not use any email address that you are not authorised to use.

Breaches of the AUP outlined in this document can sometimes result in massive numbers of e-mail responses. If any Client sends or receives so much e-mail that our resources are substantially affected, we may shut down that Client's account without notice.

4. SERVICES INVOLVING SENDING UNSOLICITED DIRECT MARKETING EMAIL

You may not operate, host or provide hosting facilities to or assist in any way whatsoever, via our Services, any web site, email address, email service, ftp service or any other online service which is advertised or promoted by means of unsolicited bulk email, unsolicited commercial email, excessive cross-posting or excessive multi-posting to Usenet newsgroups, mass messaging via mediums such as IRC, ICQ and online Instant Messaging, or any other form of electronic communication which would be regarded as defined in this AUP as being prohibited.

5. WORLD WIDE WEB USAGE

You are solely responsible for the content of Web pages owned and/or operated by you. We reserve the right to remove any Web page on our servers at any time and for any reason.

We will investigate complaints regarding inappropriate material on Web pages stored or transmitted via our Services and may, at our sole discretion, require that the material be removed or take action as outlined in Clause 6 below.

6. INVESTIGATION

We have in place a procedure for handling your complaints about material stored and/or accessed via our Services. If you wish to make such a complaint, please ensure that you make your complaint by email to abuse@visicomhosting.net. If you do not use this facility we cannot guarantee that your complaint will be dealt with promptly.

We reserve the right to investigate suspected breaches of the AUP. When we become aware of possible breaches, we may initiate an investigation, which may include gathering information from the user involved and the complaining party, if any, and examination of material on our servers. Much of the AUP reflects acts that may constitute breaches of United Kingdom legislation or regulations and may in some cases carry criminal liability.

During an investigation, we may suspend the account involved and/or remove the material involved from our servers. Such action may include temporary or permanent removal of material from our servers, the cancellation of newsgroup postings, warnings to the user responsible, and the suspension or termination of the account responsible. We will determine what action will be taken in response to a breach on a case-by-case basis.

You acknowledge that we may be required by current or future law or regulation, including but not limited to the Regulatory of Investigatory Powers Act 2000, to access, monitor, store, take copies of, or otherwise deal with your data stored on or transmitted by our Services. Without limitation, you expressly authorise us to use your personal data and other account information in connection with any such investigation, including its disclosure to any third party authority that we consider has a legitimate interest in any such investigation or its outcome.

We reserve the right to terminate Services with immediate effect and without further obligation or liability to you as required by any law enforcement authority or by the Courts.