Acceptable Use Policy
To use your Services, you must comply with this Acceptable Use Policy ("AUP").
Please Note: Unless expressly stated otherwise, terms defined elsewhere in your Agreement shall have the same meaning in this AUP.

General Information
This AUP is the result of formal and informal internet community practices and we reserve the right to amend it to ensure that it remains valid and effective. There are particular points to which you must conform when using particular Services as detailed in Appendices A to F.

It is not possible to codify exactly what constitutes "**acceptable**" and "**unacceptable**" use of our Services. Some material is illegal to possess as well as transmit or publish *via* the internet. You should not post or otherwise communicate or distribute material which infringes others' copyright or which could be considered defamatory, or which imposes liability on us for hosting that material.

Your internet traffic may traverse other networks or use services which are not owned or operated by us and you must abide by any other acceptable use policies and conditions imposed by operators of those networks and services.

We may, at our sole discretion, run manual or automatic systems to determine AUP compliance (e.g. scanning for open mail relays, open proxy servers or smurf amplifiers). By accessing the internet *via* our Services you are deemed to have granted permission for this limited intrusion onto your networks or machines.

You are required to accept email addressed to "**postmaster**" at your address. For example, if you have the hostname "**sample**" and/or the domain "**example.co.uk**", then you should accept email addressed to **postmaster@sample.demon.co.uk** and/or **postmaster@example.co.uk** respectively. You will be deemed to have read any and all such postmaster-addressed email and we may act on this basis.

If you wish to contact us in relation to this AUP, please **email: abuse@demon.net**.
If you do not use this facility we cannot guarantee that your complaint will be dealt with promptly. In addition to including a short explanation as to why you are complaining, please ensure that if reporting:
(i) email or Usenet abuse, that you provide us with a copy of the full headers of the message or article in question;
(ii) Web abuse, that you include the full URLs you are referring to;
(iii) access abuse, that you include copies of your log files highlighting the activity in question.

APPENDIX A: GENERAL INTERNET ACCESS
PLEASE NOTE: Unauthorised access to computer systems could be an offence. A list of our service machines which you may access is provided at: http://knowledgebase.demon.net/article/configuring-services.html.

While connected to the internet your system must conform to all relevant Internet Engineering Task Force ("IETF") standards.

You must not use the internet to send information packets that have forged addresses or are deliberately constructed to adversely affect remote machines.

Without the explicit permission of the relevant operators you may not run "**scanning**" software which accesses remote machines or networks.

You must ensure that you do not further the sending of unsolicited bulk email or any other form of email or Usenet "**abuse**". This applies to both material that originates on your system and also third party material passing through it.

Your machine or network must not be configured in such a way that others can exploit it to disrupt the internet. This includes but is not limited to ensuring that your network cannot be exploited as:

(i) an Open Mail Relay ("OMR") i.e. a machine which accepts mail from unauthorised or unknown senders and forwards it to a destination outwith your machine or network. Useful information can be found at: http://mail-abuse.com/an_sec3rdparty.html. If your machine performs mail relay on an authorised basis, then it must record this mail passing through your system by means of an appropriate "Received:" line.

"WinGate" users should note that this software is capable of providing a wide range of relaying services. Unless care is taken during configuration, default configurations can lead to unauthorised use.

As an exception to the relaying ban, you may run an "anonymous" relay service if you monitor it so as to detect unauthorised or excessive use. However, you may not relay traffic from such an anonymous system via our servers, i.e. you can only pass email from a system to us where this is the correct destination for final delivery.

We scan our IP Address space looking for machines that are vulnerable to unauthorised relaying, allowing us to more pro-actively prevent customers with OMRs damaging our Service.

If you have come to this page after seeing one or more of our test mails then it is very likely that your system is working correctly. You may see numerous mails because as part of our testing, we attempt to send a number of mails through your server, all with different envelope headers as different mailserver software has different types of vulnerabilities.

Further Information on how to secure various mail servers can be found at: http://www.mail-abuse.com/an_sec3rdparty.html. Queries regarding our OMR testing should be sent to: abuse@demon.net.

(ii) an Open Proxy Server i.e. a machine which accepts connections from unauthorised users and forwards their requests to a destination outside of your machine or network;

(iii) a Smurf Amplifier i.e. a router with directed broadcast enabled.

APPENDIX B: EMAIL
Most customers will apply common sense to determine what is appropriate behaviour when sending email and in so doing comply with this AUP. Regrettably, some email is sent or actions taken which are considered unacceptable by the internet community. This is usually described as "**abuse**".

It is usual to describe "**abuse**" as being abuse of internet facilities, rather than vulgar abuse sent via the internet. To qualify as "**abuse**", an act or omission must significantly interfere with network use by one or more individuals, for example by consuming resources. "**Abuse**" also includes illegal and/or dishonest activities. When abuse occurs, we will take appropriate action.

Due to "**spamming**" problems please note that sending unsolicited bulk email ("UBE"), is unacceptable. We will act when notified of such behaviour. For a first offence, education, in the form of a warning may be used, however, our policy is to terminate the Service(s) of any customer who continues to send UBE.

Chain Letters, "Make Money Fast" and other Ponzi Pyramid-Selling Schemes all constitute unacceptable abuse.

Unsolicited Commercial Email ("UCE")
UCE is advertising material sent and received by email without the recipient requesting such information or otherwise explicitly expressing an interest in such material. Please Note: simply posting a news article in any particular newsgroup, or visiting a web site does not constitute an expression of interest, unless the user specifically requested information to be emailed to them.

UBE is similar to the above UCE but is not attempting to sell anything.

Mailing List Subscriptions
Mailing lists are schemes for distributing copies of the same email to different people. It is not acceptable to subscribe anyone, other than a user on your own host, to any mailing list or similar service, without their **explicit** permission. List owners are encouraged to confirm all such requests by requesting confirmation from the apparent subscriber before starting to send any list email and must ensure unsubscribe requests are handled efficiently.

If you run a mailing list you are strongly advised to keep copies of administrative requests (web logs, or emails including headers) to demonstrate that subscription requests were genuine.

Forged Headers and/or Addresses
Forging headers or messages means sending email such that its origin appears to be another user or machine, or a non-existent machine. It is abuse to post articles with headers that would mislead recipients into believing that some other system or user had created the articles. Our systems will add header lines to try and foil such forgery, but articles will still be treated as abuse even if our actions make the attempted forgery apparent.

It is also forgery to arrange for replies to the email to be sent to other users or machines. In either case, if prior permission has been granted to you by the other user or the administrators of the other machine, then there is no problem, and of course "**null**" reverse paths can be used as defined in the relevant email standards.

Mail Bombing
Mail bombing is the sending of multiple emails, or one large email, to annoy and/or seek revenge on a fellow internet user. Please note that adding binary attachments to email may increase its size considerably.

Denial of Service Attacks
Denial of Service is any activity designed to prevent a specific host on the internet making full and effective use of its facilities. This includes, without limitation:
- Mail Bombing;
- opening an excessive number of email connections to the same host;
- sending email designed to damage the receiver's systems when interpreted; e.g. by sending malicious programs or viruses attached to an email; and/or
- using a smarthost or email relay without authorisation to do so.

APPENDIX C: USENET (sometimes called "news")
There are many forms of Usenet abuse. This appendix discusses some of the more common forms in an informal manner, but is by no means an exhaustive list.

Excessive posting
Excessive posting, commonly referred to as "**spamming**", means posting lots of substantively similar articles, usually to a large number of newsgroups. Whether the articles can be considered "**on-topic**" within the newsgroups or not is irrelevant. The Usenet community determines whether an article has been duplicated too often using the Breidbart Index ("BI"). If the applicable threshold (presently 20) is reached, postings are likely to be cancelled by systems used to detect such abuse.

Binary articles in Non-Binary Newsgroups
Binary articles contain information that is in a form not directly readable by humans, usually in "**base64**" or "**UUENCODE**" sections. These are usually "**attachments**" of images, executable files, sounds, or proprietary format documents such as Microsoft Word or Excel. Even if the attachment was originally simple text or a web page (HTML), if it has been encoded before posting it is still considered "**binary**".

Articles posted to "**non-binary**" newsgroups should contain only simple text readable without special tools. The only exception to this is the use of cryptographic authentication signatures, such as PGP. Binaries are only allowed in special binary newsgroups because this allows them to be handled by "**newsmasters**" who run Usenet's servers. To simplify matters for newsmasters, binary newsgroups are grouped together in hierarchies. Almost all binary newsgroups are to be found in alt.binaries.*, alt.sex.pictures and comp.binaries.* hierarchies.

There are also a small number of local binary hierarchies such as de.alt.binaries.*, as well as some newsgroups with special rules for particular binary types such as rec.games.bolo. Do not assume that binaries are acceptable in other groups because "**everyone posts them**" or "**nobody objects**". In particular you should note that binaries are not acceptable in any alt.fan.*, uk.* or demon.* newsgroup.

Objectionable content
Usenet is a robust medium intended for use by adults. Articles may be posted that offend or annoy other users. These may contain foul language or controversial viewpoints. The internet community does not generally consider it appropriate for content-based decisions to be made by anyone except by an individual on their own behalf. Therefore we do not consider this sort of article to be "**abuse**" and directly actionable under the AUP. If you are offended by articles made by one of our

customer's then you should arrange not to read them in the future, by using facilities provided within your newsreading software such as "**killfiles**".

None of the above is to be taken as any suggestion that you may publish material that is prohibited under local obscenity or indecency laws. For example, it is a criminal offence to even possess child abuse images in the U.K., and other content may give rise to civil actions. We do not condone the presence of this type of content anywhere on the internet. We will immediately suspend a Customer's Usenet access for this type of abuse, even if a single such article is posted.

Regrettably, articles may be posted which are considered unacceptable by the Usenet community. This is usually described by the generic term of "abuse", based on the many informal understandings that have arisen between the administrators and owners of those computers which exchange Usenet articles. This AUP and the application thereof is based on consideration of both formal and informal Usenet community practices where we are one participant among many.

There is an informal discussion of some types of material which may fall into the category of "abuse". If we consider that "abusive" articles have been posted it is important for the protection of other internet users that we take action to prevent any recurrence. If such articles were to be posted unchecked, the Usenet community could lose confidence that we will take appropriate sanctions. This could impact newsfeed peering arrangements and significantly affect the number of newsgroups and articles we can offer our customers. Consequently, we will enforce appropriate sanctions against any Customers responsible for serious abuse of Usenet including without limitation a formal warning, suspending Usenet access through our machines or access to the internet, or termination of Customer account(s).

If access suspension is imposed, we may lift it, at our sole discretion, on receipt of a formal written undertaking by the relevant customer not to post further abusive articles.

We provide access to Usenet as part of the package of internet access Services. Any decision made by us in relation to this service shall be final on all matters.

Illegal content
If you post copyright material or other intellectual property to Usenet you must have permission to do so. In particular it can be illegal to publish 'hacks' or 'cracks' of software products. It is abuse to post illegal material to Usenet.

APPENDIX D: WEBPAGES
This Appendix is applicable to all web hosting services provided by us. Appendix E gives further information applicable to Homepages services.

- **You are responsible** for your website content and must ensure that no applicable law is violated.
- **You must obtain** any necessary legal permission for any works that your website may include.
- **You will be held responsible** for and accept responsibility for any defamatory, confidential, secret or other proprietary material available via your website.

We reserve the right to remove website material at our sole discretion, without prior notice and/or explanation.

A website may not be used to offer, advertise or distribute any of the following types of material:
- illegal material;
- email address lists, except where address owners have given you explicit permission;
- any collection of personal data other than in accordance with the Data Protection Act 1998.

You must comply with the Data Protection Act 1998 (and any amendments or re-enactments of them together with any regulations pertaining thereto) regarding all information received, stored or communicated through the use of your website.

If your website contains material that may cause general offence, a clearly readable warning page must be shown before such material is displayed. To avoid doubt, this means that your top-level web page (usually **index.htm** or **index.html**) must not contain any adult material or other material that may offend. Where part of a web site forms an independent area that is not linked to by a topmost page, it will be considered as a site in its own right when considering whether appropriate warnings are present. Warnings are also required where the material is referenced directly from a website, with no intervening pages, or where the use of frames makes the material appear to be part of a website. All web pages on a website are considered to be publicly visible and may be downloaded by any person, whether or not they are linked from any central contents or home page. However, specific mechanisms are available as part of some services to prevent unauthorised access. Pages protected in such a manner will not be considered to be public.

If your website is used for "**distance selling**", you must ensure that it conforms to the requirements of The Consumer Protection (Distance Selling) Regulations 2000 (as amended from time to time) as well as all other applicable legislation.

Websites may not be advertised by you, or by another person, using techniques that would be classified as "**abuse**" if they were carried out from an account which you have with us including, but not limited to, bulk emailing and excessive news posting. Such action will be treated under this AUP as if it had been done from your account with us.

APPENDIX E: HOMEPAGES SERVICE
This Appendix gives further guidance about the Homepages service which is a web site hosting service provided as part of other services. Termination of that other service will automatically result in termination of the corresponding Homepages service. Details of technical service restrictions are available at: http://knowledgebase.demon.net/category/technical-support/hosting/homepages-webspace/.

You must not cause your pages to be accessed by any means other than in the form "www.sample.demon.co.uk" (for the hostname "sample") nor register your web pages anywhere using any form of URL except in the form beginning: http://www.sample.demon.co.uk/....

Specifically, you must not reference or cause your Homepages to be referenced by dotted IP address (e.g. [194.222.255.254]).

Should the automated enforcement of any Condition of Use or Technical Restriction fail to operate for any reason, we reserve the right to remove files from your site to apply the requirement or to require you to immediately correct the situation.

You must maintain an index page called "**index.htm**" or "**index.html**" in the root directory of your Homepages space. We will require sites that are considered to show excessive use to be modified or be moved to a different server. Excessive use is currently defined at:
http://knowledgebase.demon.net/category/technical-support/hosting/homepages-webspace/bwusage.html%20.

We reserve the right to vary the definition of '**excessive use**' at our sole discretion at any time without prior notice. We also reserve the right to make a charge for any assessment of suspended sites.

- As an exemption to the general obligation in relation to selling on or sharing use of the service, commercial use of your Homepages space is permitted.
- Helpdesk support is only available for uploading, downloading and viewing pages. No support will be given for HTML authoring or page design. A self-help newsgroup demon.homepages.authoring is available for this purpose.
- You are responsible for retaining copies of your own data. We will not keep backups of your pages.
- We accept no responsibility for loss of data, information in any form or other matters whatsoever that result from the use of this service.
- We are not liable for any loss however occasioned as a result of the suspension, removal or unavailability of a Homepages site or material stored therein.
- You may use up to a maximum of 20Mb of space. If you attempt to upload a file that exceeds your available free space the upload will normally fail. Should this check not operate for any reason, we reserve the right to request that you immediately remove enough files to bring you below the limit.
- No user defined CGIs are permitted.
- We accept no responsibility for hit counts being reset or incorrect.
- You are responsible for the content of your Homepages site, including obtaining the legal permission for any works they include and ensuring that the contents of these pages do not violate English and/or Scottish law.
- You are responsible for and accept responsibility for any defamatory, confidential, secret or other proprietary material available via your Homepages site.
- If you do not keep the index file (index.htm or index.html) in the root directory of your Homepages space for 6 weeks, the hostname (www.hostname.demon.co.uk) may be withdrawn and your Homepages site may be deleted.
- If your account is barred for any reason (e.g. non-payment) access to your Homepages site may be suspended.
- When you close your account, your Homepages site will be deleted.
- We reserve the right to remove any material from the Homepages service at our sole discretion, without prior notice and without explanation.
- The file name "bwusage.txt" (all lower case) is a reserved file name and will appear in the root directory of those Homepages sites that use more than 1Mbyte of bandwidth on any day. The complete explanation of this file is listed at **http://knowledgebase.demon.net/category/technical-support/hosting/homepages-webspace/bwusage.html%20**.
- The IP address that may be allocated to your Homepages site may be changed or withdrawn at any time without notice. It is intended to withdraw all IP addresses associated with Homepages as soon as practical.

Appendix F: Fair Usage Policy ("FUP")
The FUP* applies to Demon Business 2000, Demon Business 8000, Demon Business 2+, Demon Business 2+ Pro, Demon Business Lite +, Demon Business Lite, RSL Demon Business 2000, RSL Demon Business 8000 RSL Demon Business 2+, RSL Demon Business 2+ Pro, RSL Demon Business Lite + & RSL Demon Business Lite products and variants of these products Customers only. It does not apply to Demon Business Unlimited or Premier Broadband customers.
It is in place to ensure that we can continue to provide an acceptable standard of service in terms of download speeds, to the vast majority of our customers.

We continually measure the performance of our services and take steps to restrict usage during peak periods which may contribute significantly towards the risk of a reduced quality of service being experienced by the majority of our broadband customers. The peak period of 9am to 11pm applies to Demon Business Lite +, Demon Business Lite, RSL Demon Business Lite + & RSL Demon Business Lite. For Demon Home 8000, Demon Home 2+, RSL HomeOffice 8000, RSL HomeOffice 2+, Demon HomeOffice 8000, Demon HomeOffice 2+, Demon Business 2+, Demon Business 2+ Pro, RSL Demon Business 2+ & RSL Demon Business 2+ Pro, the peak period is between 8am & 11pm. The peak period may be subject to change dependent on usage patterns across the network.

Usage will be monitored on a continuous basis. Customers that exceed the permitted data download over a rolling 30 day period will be affected by the FUP. This is currently defined as per the limits detailed below, although we reserve the right to amend these limits in accordance with the terms of your Agreement.

Permitted data download over rolling period of 30 consecutive days
Home 8000 - 50GB of total data download.
HomeOffice 8000 - 60GB of total data download.
Home 2+ = 50GB of total data download
HomeOffice 2+ & RSL HomeOffice 2+ = 60GB of total data download
Business 2+, Business 2+ Pro, RSL Business 2+ & RSL Business 2+ Pro = 200GB peak
Business 2000, Business 8000, RSL Business 2000 & RSL Business 8000 = 100GB peak
Business Lite & RSL Business Lite = 200GB peak
Business Lite + & RSL Business Lite + = 60GB peak

We expect that less than 1% of our customers will be affected by the FUP. Any Customers who are affected will be notified via email if their speed is being restricted. Where possible, we will always endeavour to provide advance notification by email to Customers approaching the limit**

Speed restrictions will only apply during peak periods. Should a Customer's usage return to acceptable levels, adjudged on a rolling 30 day period, speed restrictions will be removed.

A practical guide to the FUP can be found at **Fair Usage Policy FAQ**.
* Unless expressly stated otherwise terms used in the FUP shall have the same definition as per the Conditions for Demon's ADSL Product Range.
** In certain circumstances, it may be possible to exceed the limit in an extremely short period of time (e.g. 24-48 hours) and in such circumstances, you may not be notified in advance of the speed of your service being restricted.