XL TELECOM - ACCEPTABLE USE POLICY

To use XL TELECOM's Internet products and services, you must comply with the provisions of this Acceptable Use Policy ("AUP") at all times. Please note that in this AUP "we"/"us"/"our/"XL Telecom" as THE GLOW XL GROUP T/As XL Telecom Limited, company number 07657964, registered office Wye View House, Bigstone Meadow, Tutshill, Gloucestershire, NP16 7JU and "you"/"your" denotes you the customer or your agent.

GENERAL

This AUP applies to every XL TELECOM Internet product and service and your use of them. For some products and services there are particular points to which you must conform when you are using that product or service. Appendices A through E of this document give further guidance as to how this AUP is applied to specific XL TELECOM Internet products and services. It is your responsibility to ensure your compliance with all applicable provisions of this AUP. If you have any comments or queries, or there is any provision that you do not understand, please feel free to email us any enquiry at abuse@xltelecom.co.uk

- You must not use your XL TELECOM product/service for any illegal purpose.
- Your traffic over the Internet may traverse other networks, or use other services, which are not owned or operated by XL TELECOM. You must abide by the relevant acceptable use policies and other terms and conditions imposed by the operators of those networks and services.
- XL TELECOM may, at its sole discretion, run manual or automatic systems to determine compliance with this AUP (e.g. scanning for open mail relays or "smurf" amplifiers). By accessing the Internet via XL TELECOM services such as a leased line, ADSL or dialup account, you are deemed to have granted permission for this limited intrusion onto your networks or machines.
- You must only send IP packets, which have a source address originating within any ranges of IP addresses for which we have agreed to provide you with connectivity
- You are required to accept email addressed to "postmaster" at any email domain we allocate to you or maintain on your behalf. For example, if you have the domain "example.co.uk", then you should accept email addressed to postmaster@example.co.uk respectively. You will be deemed to have read any and all such postmaster-addressed email. XL TELECOM may take action on the basis of this assumption.
- You are required to accept email addressed to "abuse" at any email domain we allocate to you or maintain on your behalf. For example, if you have the domain "example.co.uk", then you should accept email addressed to abuse@example.co.uk respectively. This will allow us and other Internet users to contact you directly regarding any possible breaches of this AUP. You will have been deemed to have read any and all such abuse-addressed email and taken suitable action upon it. XL TELECOM may take action on the basis of this assumption.
- Your usage of the Internet must conform to community standards. It is not possible to codify exactly what constitutes "acceptable use" and "unacceptable use" or abuse of the Internet. These terms depend upon the many informal understandings which have arisen between the administrators, owners and operators of the computers and networks that together constitute the Internet, and of which XL TELECOM is only one participant among many.

However, XL TELECOM's relationship with other networks, and ultimately its connectivity to the rest of the Internet, depends largely upon proper behaviour by its customers. XL TELECOM cannot tolerate any behaviour by customers which negatively impacts upon its own equipment or network, or upon the use by other users of the Internet, or which damages XL TELECOM's standing and reputation in the wider Internet community.

Therefore, it is important that when activity that might constitute abuse occurs XL TELECOM takes appropriate action - if it did not, and such abuse was permitted to continue XL TELECOM would lose the confidence of the wider Internet community, which in turn would significantly impair XL TELECOM's customers' freedom to use the Internet.

This AUP and its day-to-day application by XL TELECOM are a result of XL TELECOM's consideration of both the formal and informal practices of the Internet community.

The Appendices to this AUP are intended to assist customers in understanding the types of issues that can arise and what XL TELECOM will consider to be unacceptable behaviour that does not conform to community standards. These appendices are not an exhaustive list and some behaviour may still be unacceptable even if it does not exactly match some point within them.

We will investigate suspected or alleged breaches of this AUP and in doing so we will endeavour to act reasonably and fairly at all times. If you are found to have breached this AUP or the Conditions of Use or Terms and Conditions that apply to your service, we reserve the right in our sole discretion to take whatever measures we deem appropriate and proportionate to the breach. These measures may include a formal warning, suspending or terminating one or more of your XL TELECOM accounts, making an additional charge for our reasonable costs of investigating and dealing with the misuse, and/or blocking access to any relevant component(s) of our service to you. If we take such action then we may partially or fully restore your service, at our sole discretion, when the reason for our action has been addressed to our satisfaction; this may require a formal written undertaking from you not to commit any future "abuse". All cases are, however, considered individually upon their merits.

Without limitation, you expressly authorise us to use your personal data and other account information in connection with any such investigation, including by disclosing it to any third party whom we consider has a legitimate interest in any such investigation or its outcome and a reasonable need to receive the data in question.

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

The appendices refer in some cases to external web sites. XL TELECOM is not responsible for the content of these web sites. If you need any further information regarding this AUP, then please contact us on:

email: abuse@xltelecom.co.uk
fax: 03300 220001

APPENDIX A: GENERAL INTERNET ACCESS

* Some material is illegal to possess or transmit. You should also be aware that unauthorised access to computer systems could be an offence. Although many machines are connected to the Internet for general access, it does not follow that you may access any computer system you come across. Furthermore, permission to access a machine for one purpose is not implicit authority to access it for other purposes.

* Whilst connected to the Internet your system must conform to all relevant IETF (Internet Engineering Task Force) standards. The IETF standards are a subset of the RFC (Request for Comments) collection and can be found at: ttp://ftp.demon.co.uk/pub/mirrors/internic/rfc/std/

* You must not send information packets onto the Internet that have forged addresses or which are deliberately constructed so as to adversely affect remote machines.

* You must not run "scanning" software which accesses remote machines or networks, except with the explicit permission of the operators of those 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 that may pass 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 a "smurf amplifier". For more information about "smurf" attacks see:

http://users.quadrunner.com/chuegen/smurf.cgi and
http://netscan.org

* We may filter your outgoing network traffic to prevent certain kinds of abuse. If so, we will document such filtering by email to you. Such filtering will be designed not to impact legitimate use of the service. Even where such filtering is in place, you remain responsible for keeping to the terms of this AUP.

We reserve the right to restrict incoming or outgoing service in any way that we consider reasonable in order to counter DOS attacks on a server.

* You must not run an "open mail relay", that is, a machine that accepts mail from unauthorised or unknown senders and forwards it onward to a destination outside of your machine or network. If your machine performs mail relaying on an authorised basis, then it must record this mail passing through your system by means of an appropriate "Received:" line.

Please note that users of "WinGate" should take special note that this software is capable of providing a wide range of relaying services. Default configurations can lead to unauthorised use, so that special care must be taken to configure it to prevent such use. More information is currently available at:

http://www.deerfield.com/wingate/secure-wingate.htm
http://www.cert.org/vul_notes/VN-98.03.WinGate.html

* As an exception to the ban on relaying, you may run an "anonymous" relay service provided that you monitor it in such a way as to detect unauthorised or excessive use. However, you must not relay traffic from such an anonymous system via XL TELECOM's servers, i.e.: you can only pass email from such a system to XL TELECOM where this is the correct destination for final delivery.

APPENDIX B: EMAIL

There are many forms of email abuse. This appendix discusses the more common forms in an informal manner, but is by no means an exhaustive list.

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 must potentially significantly interfere with the use of the network by an individual or group of individuals in some specific way, for example by consuming resources or wasting others time. The term "abuse" also includes activities that are illegal or dishonest.

Generalities aside, due to the practical problems caused by "spamming" XL TELECOM wishes to make it clear that it considers the sending of bulk unsolicited email, of any kind, to be unacceptable behaviour. XL TELECOM will always act when such behaviour is brought to its notice. Education, in the form of an email warning, can be the most appropriate response to a first offence, since customers can be unaware of contemporary standards. However, it is XL TELECOM's policy to terminate the accounts of any customer who continues to send bulk unsolicited email.

Chain Letters, "Make Money Fast" and other Ponzi Pyramid-Selling Schemes

These articles are similar to paper versions, where you add your name at the end of a list and send the message to lots of your friends. The person at the head of the list is typically sent some small amount of money and hopes to become rich. Simple mathematics shows why they do not work in theory, and a little thought about human nature will show you why they do not work in practice either.

Other articles may ask you to send a message on to as many people as possible in order to promote some worthy cause. They are seldom anything more than hoaxes and even when originally genuine they are often no longer timely. In particular, claims of a tracking mechanism, which will ensure a good cause receives money for every copy sent, will be entirely bogus. There is no such mechanism and we are unaware of any such offer being made by any legitimate organisation.

These schemes, even where they offer no financial or material reward are unacceptable abuse. They waste resources for Internet service providers and for the users who download them. If they do involve money they are also illegal in many countries - despite common claims to the contrary within their text.

Unsolicited Commercial Email (UCE)

Unsolicited Commercial Email is advertising material sent and received by email without the recipient either requesting such information or otherwise explicitly expressing an interest in the material advertised. Since many Internet users use a dial-up connection and pay for their online time, it costs them money to receive email. Receipt of unsolicited commercial advertising therefore costs them money and is often therefore particularly unwelcome.

It should be noted that a user has not expressed an interest by the mere act of posting a news article in any particular newsgroup, or by visiting a web site, unless of course they have made a specific request for information to be emailed to them.

Unsolicited Bulk Email (UBE)

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

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 also forgery to arrange for any replies to the email to be sent to some other user or machine.

However, in either case, if the other user or the administrators of the other machine have granted prior permission to you, then there is no problem, and of course "null" reverse paths can be used as defined in relevant email standards.

Mail Bombing

Mail bombing is the sending of multiple emails, or one large email, with the sole intent of annoying and / or seeking revenge on a fellow Internet user. It is wasteful of shared Internet resource as well as serving no value to the recipient.

Due to the time taken to download it, sending a long email to sites without prior agreement can amount to denial of service, or denial of access to email at the receiving site. Note that adding binary attachments to email may increase its size considerably. If prior arrangement has not been made, the email may be extremely unwelcome.

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, but is not limited to:

* Mail bombing an address in such a way to make their Internet access impossible, difficult, or costly.
* Opening an excessive number of email connections to the same host.
* Intentionally sending email designed to damage the receiver's systems when interpreted; for example, sending malicious programs or viruses attached to an email.
* Using a smarthost or email relay without authorisation to do so.

Mailing List Subscriptions

Mailing lists are schemes for distributing copies of the same email to many different people. It is not acceptable to subscribe anyone, other than a user on your own host, to any mailing list or similar service, unless their explicit permission has been given.

List owners are encouraged to confirm all subscription requests by requesting confirmation from the apparent subscriber before starting to send any list email. They must ensure that unsubscribe requests are handled efficiently. Good emailing list software is available that will automate both these processes.

Many reports of unsolicited bulk email turn out to be from people who were unaware that they had joined a mailing list. It is not acceptable to subscribe people to a list merely because they have visited your website or used one of your products; the person must make an explicit request to be added.

However, some reports occur because people have genuinely forgotten that they had made such a request. If you run a mailing list you are strongly advised to keep copies of administrative requests (web logs, or emails including headers) so that you may demonstrate that subscription requests were genuine.

Illegal Content

Various Acts of Parliament make it illegal to possess or transmit certain material on a public telecommunications network, such as the telephone system. It is not acceptable to send such material by email.

Breach of Copyright or Intellectual Property

If you send copyright material or other intellectual property via email you must have permission to do so from a person with the right to grant such permission.

APPENDIX C: USENET (sometimes called "news")

There are many forms of Usenet abuse. This appendix discusses the more common forms in an informal manner, but is by no means an exhaustive list;

Chain Letters, "Make Money Fast" and other Ponzi Pyramid-Selling Schemes

See Appendix B above for details of this type of abuse.

XL TELECOM will immediately suspend a customer's Usenet access for this type of abuse, even if a single such article is posted.

Excessive posting

Excessive posting, commonly referred to as "spamming", means the posting of lots of substantively similar news articles, usually to a large number of newsgroups.

It is irrelevant whether the articles can be considered "on-topic" within the newsgroups or not. The problem caused by spamming is that Usenet resources are needed to store the articles and the cost to readers of the newsgroups to download duplicates of the same message. The Usenet community determines whether an article has been duplicated too often using the Breidbart Index (BI). This index measures the breadth of any multi-posting, cross posting, or combinations of the two by calculating the sum of the square roots of the number of newsgroups each article was posted to. If that number reaches 20, then the postings are extremely likely to be cancelled by automatic systems that detect this type of 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 within the article was originally simple text or a web page (HTML), if it has been encoded before posting it is still considered to be a "binary".

Articles posted to "non-binary" newsgroups should contain only simple text that is immediately readable without special tools. The size of any encoded section is irrelevant, the fact it is encoded is what makes it unacceptable. The only exception allowed to this blanket ban is the use of cryptographic authentication signatures, such as PGP.

You should note that the posting of articles formatted as HTML is unwelcome in many newsgroups, but is not, of itself, abuse. Some software will post articles formatted both as HTML and as simple text. This is also almost universally unwelcome, but will not be treated as abuse, per se, by Demon. Common obfuscation techniques, such as "rot-13", and obscure jargon and notations are not, of themselves, "binaries".

Binaries are only allowed in special binary newsgroups because this allows them to be specially handled by the "newsmasters" who run Usenet's servers. The size of binaries, in particular, means that many systems will not wish to use their bandwidth to receive them, or will expire articles more quickly to prevent them from using excessive space. In order to make things straightforward for newsmasters the binary newsgroups are all grouped together into 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 a handful of newsgroups with special rules for particular types of binaries such as rec.games.bolo. This handful of groups is specially treated because they have gone through recognised processes to gain their limited exemptions. You should 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.

Ensuring that binary articles only appear in binary newsgroups is not just a matter of convenience for the newsmasters but is also important for individual Usenet readers. The appearance of a binary in a text-only newsgroup is usually extremely unwelcome. Besides the size of the article, which will take extra time to download, special tools will be needed to decode and handle the contents.

Forged Headers

There are several types of unacceptable behaviour involving the forgery of article headers or article addresses.

It is abuse to post articles with headers that would mislead recipients into believing that some other system or user had created the articles. Demon Internet's systems will add header lines to try and foil such forgery, but articles will still be treated as abuse even if Demon Internet actions make the attempted forgery apparent.

It is abuse to post articles with headers which would cause responses to these articles, solicited or otherwise, to be delivered to unwilling third parties, or to inappropriate or unreasonable newsgroups. In particular, it is abuse to arrange for email replies to be delivered to an email address that you have not been given permission to use by a person with the right to grant such permission.

Illegal content

Some material is illegal to possess or is made illegal to transmit by various Acts of Parliament dealing with material sent over a public telecommunications network such as the telephone system that XL TELECOM uses to provide its services.

It is abuse to post illegal material to Usenet.

If you post copyright material or other intellectual property to Usenet you must have permission to do so from a person with the right to grant such permission. In particular it can be illegal to publish 'hacks' or 'cracks' of software products.

Objectionable content

Usenet is a robust medium that is intended for use by adults. XL TELECOM's customers may post articles that offend or annoy other users. These may contain foul language, controversial viewpoints;
material that is not directly on-topic for the newsgroup or indeed commercial advertisements.

XL TELECOM does not consider this sort of article to be "abuse" and actionable under the Usenet AUP.

This is because 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, if articles made by an XL TELECOM customer offend you then you should arrange not to read them in the future, by using facilities provided within your news reading software such as "killfiles".

However, 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 pornography in the U.K. and other content may give rise to civil actions. XL TELECOM does not condone the presence of this type of content anywhere on the Internet.

APPENDIX D: CUSTOMER WEBPAGES

This Appendix is applicable to all web-hosting services provided by XL TELECOM. There are some further Appendices applicable to particular services below.

You are responsible in all respects for the content of your web site and must ensure that no applicable law is violated.

You must obtain any necessary legal permission for any works that your web site may include.

You will be held responsible for and accept responsibility for any defamatory, confidential, secret or other proprietary material available via your web site.

XL TELECOM reserves the right to remove any material from a web site at our sole discretion, without prior notice and without explanation. A web site must not be used to offer, advertise or distribute any of the following types of material:

* software for sending 'spam' (bulk emails, excessive news postings, etc.);
* illegal material
* lists of email addresses, except where all the owners of the addresses 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 it) regarding all information received, stored or communicated through the use of your web site.

If your web site contains material that may cause general offence, a clearly readable warning page must be shown before any such offensive 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 generally 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 web site, with no intervening pages, or where the use of frames makes the material appear to be part of a web site.

All of the web pages on a web site 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.

Web sites must not be advertised by you, or by another person, using techniques that would be classified as "abuse" if they were carried out from an XL TELECOM account. This includes, but is not limited to, bulk emailing and excessive news posting. Such action will be treated under the XL TELECOM AUP as if it had been done from the XL TELECOM account.

Web sites must display a valid, up-to-date email contact address for the person responsible for the site. The use of the generic address of "webmaster" is acceptable for this purpose. This address must appear on the top-level page or be easily locatable from the top-level page.

APPENDIX E: BGP TRANSIT SERVICE

This Appendix is applicable to all BGP Transit services provided by XL TELECOM.

All exchange of routes between XL TELECOM and you will be via BGP4. AS numbers used in BGP4 sessions and in ASPaths in routes announced by you to XL TELECOM shall not be from ranges reserved for private use.

All routes advertised by you to XL TELECOM shall be aggregated as far as possible. You will only announce and XL TELECOM will only accept routes which are set out in a Routing Schedule agreed in advance by both parties, as amended from time to time by written agreement between the parties and any changes to the Routing Schedule will be implemented by XL TELECOM within 30 days of such written agreement. XL TELECOM will only accept routes where an appropriate route object exists in the RIPE database or equivalent Internet routing registry. You will only send IP packets to destinations, which are included in routes, which XL TELECOM has announced to you.

An excessive rate of change of reachability information for BGP routes is seen as having a detrimental effect on our network and third party networks. We reserve the right to implement industry best practice to mitigate these effects such as by using BGP Route Flap Damping (a form of which is described in the IETF document RFC2439).