

Use of Networks and the Internet in General

- You must not use the service for the transmission of illegal material. The user agrees to refrain from sending or receiving any materials which may be deemed to be offensive, abusive, indecent, hard-core or paedophile pornography, defamatory, obscene, menacing or otherwise as prohibited by current and future statutes in force. The user agrees to refrain from sending or receiving any material which may be in breach of copyright (including Intellectual Property Rights), confidence, privacy or other rights.
If you are in any doubt as to the legality of what you are doing, or propose to do, you should either take independent legal advice or cease that usage.
- You should be aware that the storage, distribution of or transmission of illegal materials may lead to investigation and possible prosecution by the UK authorities.
- You must not gain or attempt to gain unauthorised access to any computer systems for any purpose. In addition to being a breach of this AUP, such action may lead to criminal prosecution under the Computer Misuse Act.
- You must not send data to the internet using forged addresses or data which is deliberately designed to adversely affect remote machines (including but not limited to denial of service, ping storm, trojans, worms and viruses).
- You must ensure that local PCs and network connected servers are not configured to allow open relay and must not participate in the sending of unsolicited commercial or bulk email (commonly referred to as 'spam' or 'UCE') including hosting or allowing the hosting of sites or information that are advertised ('spamvertised') by UCE from a third party network or supplier.
- You are prohibited from running 'port scanning' or other software intended to probe, scan, test the vulnerability of or access remote systems or networks except in circumstances where the remote user has given express permission for this to be done.
- You may not divulge your network passwords to third parties and should take all reasonable steps to ensure that such information remains confidential.

Email

Sending and receiving email involves the same responsibilities and approach as would be used when sending or receiving any other form of communication – written or printed mail, fax, telephone call etc. Most users fully understand what would be considered appropriate and acceptable when

communicating with others and apply these considerations to their use of email. There are occasions when some users send mail or engage in online communication that others consider unacceptable – generally regarded as abuse by the online community.

If you find it difficult to determine what might be considered 'abuse' with online communication you should realise that, in general terms, anything that might be unacceptable, and possibly illegal, in other forms of communication will be equally unacceptable and possibly illegal online.

- You should not send emails that might cause annoyance, inconvenience or anxiety to a recipient.
- You should not send any emails likely to cause distress or any material which is offensive, indecent, obscene, menacing or in any way unlawful
- You must not use 4Com mail services or network to send email to any user who does not wish to receive it.
- You must not use 4Com mail services or network to send unsolicited commercial email, in bulk (commonly known as 'spam') or individually.
- You must not use 4Com mail services or network with intent to deprive others of service (e.g. 'mail bomb')
- You must not use false mail headers or alter the headers of mail messages in such a way as to conceal the identity of the sender.
- You must not use any email address that you are not authorised to use.
- You must ensure that any email servers connected to the 4Com network and operated by you are not configured to allow 'open relay'.

Customers who abuse the 4Com email service will be notified that their behaviour is unacceptable and may have their accounts suspended, terminated or blocked.

The Company reserves the right to restrict or block internet traffic to or from a Customer server, without prior notification, in the event of a failure to abide by the published terms of the Acceptable Use Policy. This may include, but not exclusively, the transmission of unsolicited email or the presence of an open mail relay.

If a customer account or service is suspended or blocked due to abuse, then service may be restored at 4Com's sole discretion and generally will only be restored on receipt of a written assurance of future compliance with this Policy and on payment of an administrative charge for restoration of service.

post.4Com-broadband.co.uk

post.4Com-broadband.co.uk is a shared SMTP relay service for 4Com's customer base. As such, in order for 4Com to provide the best level of service for all users of this system at all times, the below conditions must be adhered to by every user. post.4Com-broadband.co.uk is pro-actively administered

and 4Com work closely with other email providers to limit the amount of SPAM¹ relayed through the system.

- Sending of SPAM¹, or any otherwise offensive/abusive and/or illegal email through the system is prohibited and may result in 4Com blocking the offending IP address/Whole IP range.
- Bulk Email² is not advised and 4Com reserve the right to administratively block any sender's IP address and/or IP range that may be abusing the system in this way.
- A limit of 25 recipients per email message exists, to reduce the possibility of compromised computers sending to large numbers of invalid recipients. This action is taken to help prevent post.4Com-broadband.co.uk from being blacklisted³ by other email providers, causing inconvenience to other users of the system.
- Customers are responsible for keeping their computers/network software up-to-date and free from spyware/malware/bots etc. This can be done by running regular antivirus/antispam scans, ensuring adequate firewalling is in place (both hardware and software) and making sure all recommended Operating System patches are installed.
- Customers are advised against using the mailserver.4Com.ltd.uk cluster as a 'smarthost'⁴. Customer-managed email servers are often subject to high volume traffic, which the system is not designed for.
- Customers are advised to rate-limit⁵ emails sent out and send out-of-hours when possible.
- 4Com reserve the right to block, without notice, the IP address and/or whole IP range of any offending customer network on the mailserver.4Com.ltd.uk system if administrators deem it necessary to protect the system from degraded performance or being blacklisted by other providers.
- Any blocked IP address will be subject to a minimum of 24 hours blocking and will require a release fee⁶ to be removed.
- Repeat offences are liable to service suspension or termination. A compromised computer/network will not be considered a valid reason against such action.

¹SPAM – Unsolicited email (also UBE, UCE, Unsolicited Bulk Email/Unsolicited Commercial Email). This is unwanted 'junk' email', usually advertising products or containing illicit or otherwise illegal material.

²Bulk Email – (Also 'Mass Mail') refers to a large volume of email sent out at any one time. This is usually to a large number of recipients, either numerous recipients per email envelope, or hundreds of recipients in separate emails. Bulk Email also refers to a large number of mails sent within a small timeframe.

³Blacklisted – Email servers may 'blacklist' another provider's mail server if it's seen to be sending lots of junk email. This prevents any other users on that server from sending email to domains hosted by the blacklisting server. This obviously causes large inconvenience for all users, so needs to be avoided.

⁴Smarthost – This is the process of relaying mail from a customer's own mail server via mailserver.4Com.ltd.uk. The preferred method of email delivery is to send directly via SMTP.

⁵Rate-limit – If sending to multiple recipients, emails should be sent at a rate of no more than a few emails per minute.

⁶Release Fee – A payment of £100 + VAT will be required. An email or signed fax from a registered contact stating that the issue causing the problem has been resolved and that the fee has been accepted will be required before the block can be lifted.

Web Usage

Web usage includes the use of web space provided with client accounts, web hosting on 4Com servers and the use of web services and space on customer colocated servers.

4Com cannot and does not proactively monitor content on any web space maintained by customers (whether customer space, web hosted or colocated services) and cannot and does not guarantee that such sites are free of illegal content or other materials that may be considered unacceptable.

- You undertake sole responsibility for the content of web pages owned and or operated by you – whether on client pages, web hosted space or colocated servers.
- You undertake sole responsibility to ensure that all materials on any web site owned or operated by you contains material that you have created or have permission to use.
- You undertake sole responsibility for any dispute involving Copyright or Intellectual Property Rights associated with your site or service.
- You must not use your website or web service to promote or distribute any material or content that is illegal (under any current or future legislation). You should be aware that the internet is a global communications network and what may be legal in the UK may be illegal elsewhere and leave you liable to prosecution in another country.
- You must not host or allow the hosting of sites or information advertised ('spamvertised') by UCE, including UCE from third party network(s) or supplier(s).

4Com may undertake investigation of content services if potential abuse is brought to its attention and reserves the right to remove any web page on our servers at any time and for any reason.

Abuse of 4Com Services

Please address all complaints about abuse of services to abuse@4Com.co.uk

4Com reserves the right to investigate suspected or potential abuse of its Acceptable Use Policy. If we become aware of possible abuse, either through our own investigations or through referral by another user or by a third party, we may begin an investigation that may include gathering information from all potential parties and materials on our servers. 4Com reserves the right to suspend accounts or access during such investigations and/or to remove materials from servers (on a temporary or permanent basis). All actions will be determined on an individual basis and will not be taken to form any precedent.

4Com customers who engage in abuse of the network and/or the internet will be notified that their behaviour is unacceptable and may have their accounts suspended or terminated. If a customer account or service is suspended or blocked due to abuse, then service may be restored at 4Com's sole discretion and generally will only be restored on receipt of a written assurance of future compliance with this Policy and on payment of an administrative charge for restoration of service. All 4Com users acknowledge that the Company may be required by current or future legislation to access, store, copy or otherwise Customer data stored within or transmitted by our service. By accepting this Acceptable Use Policy you expressly agree that we may access and use your personal data or other account information in connection with any such investigation and may disclose such data to any third party who has a legitimate interest in the data, investigation or outcome. 4Com reserves the right to terminate service, with immediate effect and without further obligation or liability to Customers, as required by any law enforcement authority or by the Courts of the United Kingdom.

Regulation of Investigatory Powers Act 2000, Terrorism Act 2006

4Com undertakes to take action required under the provisions of the Regulation of Investigatory Powers Act 2000, Terrorism Act 2006 and or other relevant legislation and will fully cooperate with the appropriate UK authorities