

## 1. Introduction

For the internet to operate in a manner that satisfies the majority of its users, all users need to observe some rules and etiquette governing their use of it. These requirements are usually contained or referred to in the relevant terms and conditions governing the particular internet service as well as general law.

Alpha Technology System Ltd customers must ensure that they know what these requirements are and how they are affected by them.

To enable its customers to have a better understanding of what is and is not acceptable when using the internet, and to help you get the best out of the internet, Alphatech has developed a number of Acceptable Usage Policies (AUPs) relating to internet services. Complying with these AUPs, which is a contractual requirement, should help you benefit from safer surfing and minimise the risk of suffering "online abuse".

Alpha Technology System Ltd AUPs are based on current "best internet industry practice" and draw on the collective experience of users and service providers across the internet community.

We may change the AUPs from time to time. To make the most of the guidance contained in the AUPs, please keep up to date with changes and look at them on a regular basis. We hope you will find them useful and informative.

## 2. A Guide To Avoiding Abuse While Connected To The Internet

### Common Sense

The majority of Alpha Technology System Ltd online customers will be using commercial software to connect to and navigate the internet. This software implements the technical aspects of the connection but there are also some simple common sense checks which all customers can implement. For example, making sure that the computer is dialling the whole number, including the area code, will reduce the possibility of other people receiving unwanted calls.

### Legal Compliance

The internet is a global medium and is regulated by the laws of many different countries. Material which is illegal in this country may be legal in another, and vice versa. As a user in this country, for example, you should not access sites carrying child pornography, hard-core pornography or incitement to violence. These are just three examples of unlawful material and there are many others. When you visit a website, a copy of the visited pages is stored on your pc in the web browsers' cache files. Storage of illegal material in this way may well constitute a criminal offence. If you are in any doubt, we recommend you to take independent legal advice.

To connect to any of Alpha Technology System Ltd online services, you will use a telephone (PSTN) line, ISDN line or ADSL. While connected to the internet, you must comply with legal requirements concerning telephone network (mis)use. Set out below is a self explanatory extract from the Telecommunications Act. As you can see, network misuse is a serious criminal offence which can lead to fines and/or imprisonment.

### "Improper Use Of Public Telecommunication System"

- A Person who -
  - sends by means of a public communication system, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character, or
  - sends by those means, for the purpose of causing annoyance, inconvenience or needless anxiety to another, a message that he knows to be false or persistently makes use for that purpose of a public telecommunication system, shall be guilty of an offence and liable on summary conviction to imprisonment for a term not exceeding six months or a fine..... or both".

### **Avoiding Abuse While Connected To the Internet**

Taking the following steps should help you to protect yourself from becoming a victim of abuse while connected to the internet:

Ensure that you are running a good quality virus detection application. The majority of these applications have the ability to detect hackers as well as viruses. Hackers are people who try to hack into your computer to either cause mischief or find your passwords and usernames. You should be aware that some hackers have the ability to seriously damage your computer system!

If you keep sensitive information on your computer, it is worth using encryption software to protect it.

While connected, do not publicise your IP address. This is the unique ID that your ISP allocates you while you are connected to the internet. This is especially important if you are using applications such as CHAT, IRC (internet relay chat) or video conferencing using a directory service.

A majority of people spend their online time finding internet software applications to run while online. Be careful what you install. Before installing software of unknown origin, ask yourself whether you trust the writer/source. Most computer viruses and Trojans are installed unknowingly while installing shareware or freeware applications that are supposedly designed to make your life easier. If in doubt, don't do it!

### **Sharing Logon Details**

Alphatech prohibits customers from sharing details.

### **Port Scanning**

Alphatech prohibits the use of port scanning software on its services.

### **Sharing Internet Access on a Private Network and Running Personal SMTP Mail Servers**

Some methods of sharing internet access or applications expose your external internet connection to other internet users, and enable them to send unsolicited bulk emails via your computer (known as SPAM).

As Alphatech do not block any ports it is vital that you configure your network securely, you are fully responsible for security in your own network and failure to secure it properly will result in your disconnection from Alphatech services.

## **3. Internet Access - Acceptable Use Policy (AUP)**

### **Introduction**

Alpha Technology System Ltd relationships with its customers, other networks, and ultimately its connectivity to the rest of the internet, require its customers to behave responsibly. Accordingly, Alphatech cannot permit irresponsible behaviour by its customers, which could damage these relationships, Alpha Technology System Ltd network or the use of the internet by others.

Compliance with this Acceptable Use Policy is a contractual requirement. If you fail to do so, your service may be suspended or terminated.

### **Heavy Usage**

Persistent heavy users of the service, who in Alpha Technology System Ltd reasonable opinion could be seen to be over-using their contended service, may at Alpha Technology System Ltd discretion find their available bandwidth restricted at certain times of the day.

### **Partners:**

- Managed Whitelabel
- Unmanaged L2TP (Standard based charging)

Data Transfer: 50GB per month

Exceeders either:

- Move to PAYG platform where available.
- Move into restricted daytime context\*
- Move to SDSL where available.

#### Data Transfer Above: 100GB per month

Exceeders either:

- Move to PAYG platform where available
- Move into restricted all hours context\*\*
- Move to SDSL where available.

#### **\*Restricted Daytime Context**

- Contended 50:1 during business hours 0800 - 1800.
- No restrictions outside of these hours.
- Any user exceeding the 100GB limit will be put into the restricted all hours context\*\*

#### **\*\*Restricted all hours context**

- Contended 50:1 24/7/365.

#### **Appeals**

50GB Exceeders: Business cases where one line is part of a multi site VPN or similar will be considered, traffic profiles and type will be taken into consideration. The data transfer of the combination of sites must not exceed 50GB per site. Non business traffic users will have to remain in the restricted daytime context.

100GB Exceeders: Business cases where one line is part of a multi site VPN or similar will be considered, traffic profiles and type will be taken into consideration. The data transfer of the combination of sites must not exceed 50GB per site .

Please email [support@alphatechonline.co.uk](mailto:support@alphatechonline.co.uk) to register an appeal against our decision.

#### **Alphatech customers:**

- Alphatech Direct or Reseller

#### Data Transfer: 50GB per month

Exceeders either:

- Move to SDSL where available
- Move into restricted daytime context\*

#### Data Transfer Above: 100GB per month

Exceeders either:

- Move into restricted all hours context\*\*
- Move to SDSL where available

### **\*Restricted Daytime Context**

- Contended 50:1 during business hours 0800 - 1800.
- No restrictions outside of these hours.
- Any user exceeding the 100GB limit will be put into the restricted all hours context\*\*

### **\*\*Restricted all hours context**

- Contended 50:1 24/7/365.

### **Appeals**

50GB Exceeders: Business cases where one line is part of a multi site VPN or similar will be considered, traffic profiles and type will be taken into consideration. The data transfer of the combination of sites must not exceed 50GB per site. Non business traffic users will have to remain in the restricted daytime context.

100GB Exceeders: Business cases where one line is part of a multi site VPN or similar will be considered, traffic profiles and type will be taken into consideration. The data transfer of the combination of sites must not exceed 50GB per site .

Please email [support@alphatechonline.co.uk](mailto:support@alphatechonline.co.uk) to register an appeal against our decision.

### **Illegal Activities**

You must not, by using the service, possess or transmit illegal material. You should be aware that as the internet is a global network, some activities/material which may be legal in the UK, may be illegal elsewhere in the world and vice versa. When you visit a website, a copy of the visited pages is stored on your pc in the web browsers' cache files. Storage of illegal material in this way may well be a criminal offence, as well as contravening this AUP.

If you are in any doubt as to the legality of anything, don't do it and take independent legal advice before proceeding.

You must not gain or attempt to gain unauthorised access to any computer systems for any purpose, including accessing the internet. As well as being in breach of your contract for the particular service, such hacking or attempted hacking is a criminal offence.

### **Forging Addresses**

You must not send data via the internet which has forged addresses or which is deliberately constructed to adversely affect remote machines. You must not configure your pc as an open relay system.

### **Port Scanning**

You must not run "port scanning " software which accesses remote machines or networks, except with the explicit prior permission of the administrator or owner of such remote machines or networks. This includes using applications capable of scanning the ports of other internet users.

If you intend to run a port scanning application, you must provide Alphatech with a copy of the written consent received from the target of the scan authorising the activity. This must be supplied to Alphatech prior to the application being run.

### **Spam or Unsolicited Email**

You must not participate in the sending of unsolicited bulk email or any other form of email or Usenet "abuse". This applies to material which originates on your system as well as third party material which passes through your system.

### **Internet Connection Sharing**

If you share the resources of your internet connection over a Private Network on your premises, you must

make sure that your network is secure, and that any internet Connection Sharing software that you are using does not permit access from outside of your network. This is especially important if running an "Open Proxy Server". This is because an "Open Proxy Server" will allow other users of the internet to exploit your internet connection, and use it as if it were their own. For example, an external user could access your local network or send unsolicited e-mail(s) that would appear to come from you.

### **What Action Will Alphatech Take?**

Compliance with this Acceptable Use Policy is a contractual requirement. If you fail to do so, your service may be suspended or terminated.

Alphatech may operate systems to ensure compliance with this AUP, including without limitation port scanning and testing of open servers and mail relays.

Customers who engage in abusive behaviour will be notified that their behaviour is unacceptable and may have their accounts suspended or terminated.

### **Account Restoration**

A suspended account may be restored at Alpha Technology System Ltd discretion, upon receipt of a written undertaking by the abuser not to commit any future "abuse". All cases are, however, considered by Alphatech on their individual merits.

### **A Guide to Avoiding Email Abuse**

Email is without doubt an extremely effective and convenient method of communication. It is fast and cheap. Unfortunately, it is also the most common source of abuse over the internet. Although much unsolicited email (SPAM) may just be a harmless but annoying way of advertising of products or services, some can be as distressing as receiving malicious telephone calls.

There are some simple steps you can take to minimise the likelihood of receiving nuisance emails:

Don't give out your email address unless you are absolutely sure you can trust the recipient. You should treat your email address as you would treat your telephone number.

When posting into newsgroups configure your newsreader so that it doesn't show or it disguises your email address, i.e. joe.bloggs32@nospam.isp.com. In the posting you would say "to reply to Joe, remove the nospam". A person responding to the email then has to remove the nospam section of the email address. This makes it more difficult for automated newsgroup trawlers to strip email addresses from the postings. The majority of the mail lists that are used for the bulk sending of emails are compiled from undisguised email addresses in newsgroups.

Avoid posting into newsgroups if you are not entirely sure about the nature of their subject matter. If you are going to post into these groups, be aware that there is very little your ISP can do to protect you if you become a victim of abusive emails resulting from your posting or a "flame war". If you do post into such newsgroups, it is a sensible precaution to keep your email address private, as often the only cure to stop nuisance emails is to change your email address.

### **Never publicise your home address or telephone number.**

Be very careful when sending details such as your credit card number by email. Unless you are completely sure you can trust the recipient and the details of the recipient's email address don't do it.

When filling in on-line forms always look for and complete any "data protection opt out" boxes if you do not wish to be contacted regarding advertisement and promotion of any products and services. The information you provide may be disclosed to other organisations or used for marketing or other purposes which you did not envisage. If in doubt, do not use the on-line form.

If you do become a victim of abusive emails, there is often very little your ISP can do to stop the abuse. However, the ISP of your abuser can possibly do something under its terms and conditions. Accordingly, we recommend you to take the following action:

- a. Email the "abuse department" for the individual's ISP.

- b. Send the relevant ISP as much evidence as possible. It is no use simply complaining about the activities of an individual, you must provide evidence of the abuse, e.g. send the whole email, newsgroup posting or the URL of the website to abuse@ the ISP in question. The ISP will probably need the IP Address that the abuser was using at the time of the abuse. This is the unique ID allocated to that user at that specific moment and can be found/seen in the header of the email, and in the header of the newsgroup posting.
- It is unlikely that an ISP will simply give out the name and details of an alleged offender. However, an ISP may need to divulge such information to appropriate authorities, such as the police or the courts, if formally requested to do so.

In cases of extreme net abuse, you may need to contact the police if you think further action should be taken. If you decide to do so, you must be prepared to provide the police with any evidence you have. The police will then consider whether a criminal offence may have been committed and whether further action can or should be taken.

#### Sharing Internet Access on a Private Network and Running Personal SMTP Mail Servers

Some methods of sharing internet access or applications expose your external internet connection to other internet users, and enable them to send unsolicited bulk emails via your computer (known as SPAM).

As Alphatech do not block any ports it is vital that you configure your network securely, you are fully responsible for security in your own network and failure to secure it properly will result in your disconnection from Alphatech services.

## 4. Email - Acceptable Use Policy (AUP)

### Introduction

Exchanging emails with others generally involves using common sense regarding the content material and being polite and courteous. The vast majority of Alpha Technology System Ltd customers understand what is appropriate when sending or receiving emails. Regrettably, there are occasions when individuals or groups of people exchange emails or involve in online activities, which are considered to be unacceptable by the internet community. This is described by the generic term of "abuse".

This email AUP is based on current "best internet industry practice" and draws on the collective experience of email users and service providers across the internet community.

### Abusive emails

It is not always obvious whether an activity is innocent, inadvertent, or intentional but as a general rule, email users should be aware that what is unacceptable (and possibly illegal) offline (oral or written), applies equally online. As with telephone calls, you must not send any emails which cause annoyance, inconvenience or needless anxiety. You should not send false messages likely to cause distress (e.g. advising the recipient that a relative has been in an accident when they have not), or any other material which is distressing, grossly offensive, indecent, obscene, menacing or in any other way unlawful. Particular care should be taken to avoid any material which is offensive to people on grounds of gender, race, colour, religion or other similar categorisation. Always be sensitive to the fact that children might have access.

### Spam (Unsolicited Bulk emails)

You must not use Alpha Technology System Ltd email system to send unsolicited emails, bulk or otherwise. The sending of such emails is an abuse of the service and you will be in breach of the relevant terms and conditions.

### **Setting up Your Mail Server (Open Relay)**

If you choose to run an SMTP email server on a private network on your premises you must ensure that it is configured correctly, so as to only accept mail from your private domain. Alphatech will block access (TCP port 25), to your SMTP email server from outside of your domain to prevent it from being exploited for the purpose of sending unsolicited emails.

### **Internet Connection Sharing**

If you share the resources of your internet connection over a Private Network on your premises, you must make sure that your network is secure, and that any Internet Connection Sharing software that you are using does not permit access from outside of your network. This is especially important if running an "Open Proxy Server". This is because an "Open Proxy Server" will allow other users of the internet to exploit your internet connection, and use it as if it were their own. For example, an external user could access your local network or send unsolicited e-mail(s) that would appear to come from you.

### **What Action Will Alphatech Take?**

Compliance with this Acceptable Use Policy is a contractual requirement. If you fail to do so, your service may be suspended or terminated.

Alphatech may operate systems to ensure compliance with this AUP, including without limitation port scanning and testing of open servers and mail relays.

Customers who engage in abusive behaviour will be notified that their behaviour is unacceptable and may have their accounts suspended or terminated if such behaviour continues.

If we find out that you are using our service for illegal purposes, we may notify the police. If we receive a Court Order requesting us to reveal your identity to someone complaining that you have used this service in an abusive manner we will do so.

### **Account Restoration**

A suspended account may be restored at Alpha Technology System Ltd discretion, upon receipt of a written undertaking by the abuser not to commit any future "abuse". All cases are, however, considered by Alphatech on their individual merits.

### **A Guide to Avoiding newsgroup Abuse**

Alphatech provides a hierarchy of newsgroups which although being unmoderated, they are subject to their own charters. These charters are posted into the newsgroups on a regular basis. Newsgroups outside this hierarchy are outside Alpha Technology System Ltd control and Alphatech has no say in the type of material that can and cannot be posted to them. Please note that Alphatech takes complaints made by and against its customers very seriously, even if they concern customers that use newsgroups outside the Alphatech hierarchy.

Alphatech aims to filter out newsgroups that are perceived by their titles to have illegal content. However, Alphatech does not monitor the content contained in any of the newsgroups and is not responsible for the content of any newsgroup. Specifically in the interest of the safety of children, Alphatech asks that if you identify a newsgroup with illegal content, you notify us as soon as possible in order that we can consider adding that group to our list of barred groups.

We recommend that you take some simple steps you can take to minimise the likelihood of receiving abuse via a newsgroup:

Do not give out your email address unless you are absolutely sure you can trust the recipient. You should treat your email address as you would treat your telephone number.

When posting into newsgroups it is wise to configure your newsreader so that it does not show or it disguises your email address, i.e. joe.bloggs32@nospam.isp.com. In the posting you would say "to reply to Joe, remove the nospam". In this event, a person responding to the email would have to remove the nospam section of the email address. This makes it more difficult for automated newsgroup trawlers to strip email addresses from the postings. The majority of the mail lists that are used for the bulk sending of emails are compiled from undisguised email addresses in newsgroups.

Avoid posting into newsgroups if you are not entirely sure about the nature of their subject matter. If you are going to post into these groups, be aware that there is very little Alphatech, as your ISP, can do to protect you if you become a victim of abusive emails resulting from your posting or a "flame war ". If you do post into such newsgroups it is a sensible precaution to keep your email address private, as often the only cure to stop nuisance emails is to change your email address.

- Never publicise your home address or telephone number.
- Do not post material that falls outside the topic under discussion. Every newsgroup has a title; the content should reflect that title.
- Do not post binary attachments, (pictures or files on your computer etc.) into newsgroups not designed for that purpose.
- You must observe copyright issues. Do not post material that you did not create, unless you have the permission of the owner of the relevant rights in that material.
- Do not post advertisements into newsgroups of a non-commercial bias.
- Be careful what you post. What may seem amusing to you may very well be offensive to another participant in the newsgroup.
- Try not to cross post (post the same article to a number of groups).

If you do become a victim of Usenet abuse, outside of the "ispNAME." hierarchy, there is often very little your ISP can do to stop the abuse. However, the ISP of your abuser can possibly do something under its terms and conditions. Accordingly, we recommend you to take the following action:

- a. Email the "abuse department" for the individual's ISP.
- b. Send the ISP as much evidence as possible. It is no use simply complaining about the activities of an individual, you must provide evidence of the abuse, e.g. send the whole email, newsgroup posting or the URL of the website to abuse@ the ISP. The ISP will most probably need the IP address that the abuser was using at the time of the abuse. This is the unique ID allocated to that user at that specific moment and can be found /seen in the header of the email, and in the header of the newsgroup posting.

It is unlikely that an ISP will simply give out the name and details of an alleged offender. However, an ISP may need to divulge such information to appropriate authorities, such as the police or the courts, if formally requested to do so.

In cases of extreme net abuse, you may need to contact the police if you think further action should be taken. If you decide to do so, you must be prepared to provide the police with any evidence you have. The police will then consider whether a criminal offence may have been committed and whether further action can or should be taken.

### **Guide to Avoiding Abusing Your Webpace**

As part of certain internet services, Alphatech offers its customers personal webpace. This is an area on Alpha Technology System Ltd internet servers that you can personalise and display to the World Wide Web (WWW).

To help you get the most from your webpace, and to avoid either infringing the relevant terms and conditions or becoming a victim of abuse because of your content, here are some simple do's and don'ts:

The support Alphatech provides relates only to accessing your webpace. Alphatech does not provide support for HTML authoring, page design or how to publish your pages. Make sure you do not display too much personal detail on your webpace and remember that you publish any personal information at your own risk.

Avoid content that can offend. If you have any doubt about the suitability of your content to others, in particular to children, you must give a warning page before reaching the content. If in doubt, seek independent legal advice.

You must not publish content, or link to, content in which you do not own the rights, without the permission of the owner of the relevant rights.

Be careful with content that may lead to argument. This is especially important if your website is also your primary email address. Remember not everyone has the same opinion as you, and what you say could be offensive to others and lead to a situation where you receive abusive e-mails.

You must not publish or link to content that is illegal. You must also remember that what is legal in this country is not necessary legal everywhere else in the world (and vice versa) and that you could risk being prosecuted in another country if what you publish is illegal in that country. If in doubt, don't do it and take independent legal advice before proceeding.

You must not incite disorder or publish any material, which would amount to instructions concerning illegal activities.

You must not publicise the personal details of others without their consent.

You must not use your website to advertise, distribute (or link to another webpage containing) virus creation software, e-mail spamming software, or port scanning software.  
Don't share the password for your webspace. Your passwords are your responsibility, and must not be disclosed to any third party. This is important for your own protection.

## **WEBSPACE - Acceptable Use Policy (AUP)**

### **Introduction**

The following AUP contains rules governing the use by customers of Alphatech webspace services.

It is based on current "best internet industry practice" and draws on the collective experience of webspace users, service providers and the owners and administrators of computer networks which are connected to form the World Wide Web.

Alphatech cannot and does not proactively monitor content on its customers websites and therefore cannot and does not guarantee that all such websites are free of illegal material or other content considered unacceptable (abusive) by the internet community.

### **Illegal Activities**

You must not have illegal material on your website or link to content that is illegal. You should be aware that as the internet is a global network, some activities/material which may be legal in the UK may be illegal elsewhere in the world and vice versa, and you could risk being prosecuted in another country if you publish what is illegal in that country. If you are in doubt, don't do it and take independent legal advice before proceeding.

You must not incite disorder or publish any material which would amount to instructions concerning illegal activities.

You must not publish content, or link to content in which you do not own the rights, without the permission of the owner of the relevant rights.

### **Unacceptable Behaviour**

It is not always obvious whether an activity is innocent, inadvertent, or intentional, but generally webspace users should be aware that what is unacceptable (and possibly illegal) offline (oral or written), applies equally online.

Avoid content that may offend. If you have any doubt about the suitability of your content to others, in particular to children, you must give a warning page before reaching the content. If in doubt, don't do it and take independent legal advice before proceeding. In particular, you must not use expressions that are offensive to others on grounds of gender, race colour, religion or other similar categories. Alphatech will not make any logs or details of who visited your site available.

- You must ensure that your index.htm or default.htm file (the first to be viewed on a site) does not contain any material liable to offend. A clearly readable warning page must be displayed before any adult material is displayed.
- You must not use your webspace to cause annoyance, inconvenience, offence or needless anxiety.
- You must not publicise the personal details of others without their consent.
- You must not use your website to advertise, distribute (or link to another webpage containing) virus creation software, e-mail spamming software, or port scanning software.
- Your homepages site may not be used to distribute or advertise any of the following:
  - Software for sending SPAM (excessive news postings, bulk emails etc.).
  - Software for port scanning, virus creation, hacking or any other illegal or antisocial activity.
  - Lists of email addresses except where all the addressees have given their explicit permission.
  - Any collection of personal data other than in accordance with all applicable data protection legislation.
  - Links to websites hosting illegal content, including adult material
  - Content designed to offend or cause needless anxiety to others.
- You must not advertise your Homepages (websites), or cause another person to advertise it, by techniques that would be classified as abuse, e.g. bulk emailing and excessive news posting.

### **Security**

You must not share the password for your webspace. Your passwords are your responsibility, and must not be disclosed to any third party. This is also important for your own protection.

### **What Action Will Alphatech Take?**

Compliance with this Acceptable Use Policy is a contractual requirement. If you fail to do so, your service may be suspended or terminated.

Offending material may be removed without prior notice/explanation. Customers who engage in abusive behaviour will be notified that their behaviour is unacceptable and may have their accounts suspended or terminated.

If we find out that you are using our web space service for illegal purposes, we may involve Alpha Technology System Ltd E-crimes and Investigations team and we may ultimately notify the police. If we receive a Court Order requesting us to reveal your identity to someone complaining that you have used this service abusively, we will do so.

### **Account Restoration**

A suspended account may be restored, at Alpha Technology System Ltd discretion, upon receipt of a written undertaking by the abuser not to commit any future "abuse". However, Alphatech will consider all cases on their individual merits.

## **5. A Guide To Using Chat And Instant Messaging Services**

Chat is carried out in a 'room'. The room usually has a theme so people can chat together about the same topic. Rooms are generally public so that anyone can join in.

Instant messaging is a way of sending text messages to other people connected to the internet

Chat and Instant Message services are great fun to use and both are tremendously popular with teenagers.

However, where there's fun there's also risk. Both these services are a potential source of worry, especially to parents, as there's no way of checking that the people in the chat room are who they say they are. In fact most chat rooms encourage you to adopt an alias. Therefore chat rooms can be used by adults who may, for example, pretend to provide a sympathetic ear for a teenager's problems, possibly coaxing personal information out of them and trying to arrange a 'real life' meeting. In addition, passions can run high online and chat rooms can easily be the scene of violent arguments.

But please don't be put off by this as there are some steps you can take to minimise risks.

- Important advice to use chat and instant message services more safely
- children under 13 years must not be allowed to use Chat or Instant Message
- children under 16 years should be supervised when using these services. Make certain they know they should never give out any personal details or details that could be pieced together so that they could be identified, e.g. name of school
- when setting up the service check to see if you can hide your IP address from other people using the service. Hiding your IP address helps protect your computer and keeps it hidden from other users
- make sure that none your personal details are available to other users. Most Chat and Instant Message services let you choose what details to share with others
- make sure your children are aware of the dangers of using this type of service
- never publicise your home address, telephone number or credit card details
- don't give out your email address or other personal details unless you're absolutely sure you can trust the recipient. Never give it out in a public chat room where anyone could be watching and make use of it. You should treat your email address as you would treat any other personal details about yourself
- if you decide to meet someone that you've been chatting with, arrange to meet in a public place and make sure that you've told a friend where you're going and who you're meeting. Better still; take a friend along with you.
- try to avoid getting into heated arguments in public chat rooms. It is best to leave the chat room if you find yourself in this situation rather than become involved

If you do become a victim of abuse in a chat room, there's often very little your ISP can do to stop the abuse. However, the Chat or Instant Message Service provider may be able to identify the abuser and forward details to their ISP who may be able to take action under its Terms & Conditions. If you do need to complain in this way, you should email as much information as you can, including all the details of your conversation (by cutting and pasting) to the Chat or Instant Message Service provider. In the case of Alpha Technology System Ltd Chat or Instant Message services, you should send your complaint to [abuse@Alphatech.com](mailto:abuse@Alphatech.com).

In cases of extreme abuse, you should contact the police if you think further action is required. If you decide to do so, you must be prepared to provide the police with any evidence you have. The police will then consider whether a criminal offence may have been committed and whether further action can or should be taken.

## **6. Chat & Instant Message Service - Acceptable Use Policy (AUP)**

### **Introduction**

Using Chat and Instant Message Services on the internet generally requires politeness, courtesy and caution in exactly the same way as face-to-face and telephone conversations. This is probably more important when communicating with strangers.

Most people understand and apply acceptable standards of behaviour and language when using these services.

However, there are times when individuals, or groups, behave in what is considered by the internet community to be an unacceptable way. This is described by the generic term of 'abuse'.

### **Conduct in Chat Rooms**

Please remember that what is acceptable by one culture may be regarded as offensive by another. Since the internet is worldwide, please take great care to avoid giving offence.

We recognise the right to freedom of expression, but with that right comes a responsibility to respect the feelings of others. It's not necessary to use inflammatory language to express strongly held views.

Abuse may be innocent, inadvertent or intentional. It's not always clear which is which, so please remember that the following are NOT allowed:

- saying anything that would cause annoyance, inconvenience or needless anxiety to other users
- advertising products or services
- using foul language
- using explicit sexual language or inappropriate behaviour
- frequently changing Username and jumping in and out of rooms ('frogging')
- making insulting remarks at other members ('flaming')
- Conduct in Instant Message Communications
- You must not use the service to:
  - distribute illegal, indecent or offensive material or any messages that may incite disorder or encourage illegal activities
  - cause annoyance, inconvenience or anxiety to other users
  - impersonate someone else
  - distribute material in which you do not own the copyright, without the permission of the owner of the relevant rights
  - transfer files that contain viruses, trojans or other harmful programs
  - distribute advertisements or junk mail ('spam')
  - Important safety advice
  - Children under 13 years must not use the service.
- We strongly recommend that a responsible adult supervises children under 16 years while they're using the service.

#### **What Action Will Alphatech Take?**

Compliance with this Acceptable Use Policy is a mandatory requirement under our Terms & Conditions. If you fail to comply, your service may be suspended or terminated. Alphatech will co-operate with providers of other Chat and Instant Message Services to identify any customers committing abuse. If we discover that you've engaged in abusive behaviour we'll notify you that your behaviour is unacceptable. Your account(s) may be suspended or terminated.

If we find out that you're using our service for illegal purposes, we may notify the police. If we receive a Court Order requesting us to reveal your identity to someone complaining that you've used this service in an abusive manner we will do so.

#### **Account Restoration**

A suspended account may be restored at Alpha Technology System Ltd discretion, upon receipt of a written undertaking by the abuser not to commit any future 'abuse'. All cases are, however, considered by Alphatech on their individual merits.

### **7. Internet Glossary**

**Applet**- A type of computer program that allows animation and other interactive functions on a file or Web page.

**ADSL** - Asynchronous Digital Subscriber Line - A new technology that allows you to access the internet over standard phone lines at very high speeds.

**Bit** - The smallest piece of digital information understood by computers.

**Bandwidth** - The rate information travels from one place to another either inside a computer or between computers. Bandwidth is usually measured in bits per second, kilobits (thousands of bits) per second, or megabits (millions of bits) per second. A 28.8 modem allows for a connection of 28.8 kilobits per second.

**Blocking software** - A computer program that allows parents, teachers, or guardians to "block" access to certain Web sites and other information available over the internet. All blocking software has filtered the information before blocking access to it. (See also "filtering software")

**Bookmark**- A placeholder for interesting or frequently used Web sites, so that these sites can be revisited easily without having to remember or retype the internet address.

**Browser** - A software product that lets you find, see, and hear material on the World Wide Web, including text, graphics, sound, and video. Popular browsers are Netscape Navigator and Microsoft Internet Explorer.

**Byte** - Bytes are a basic measurement of computer memory. A byte is made up of eight bits.

**Cache** - A cache is a place on your hard drive where the Web browser stores information (text, graphics, sounds, etc.) from pages or sites that you have visited recently so that returning to those pages or sites is faster and easier.

**CD-ROM**- A computer disk that can store large amounts of information; generally used on computers with CD-ROM drives. "CD-ROM" stands for "Compact Disk Read Only Memory". That means it can only play back information, not record or save material.

**Chat**- A feature of online services or Web sites that allows participants to "talk" by typing messages that everyone can read at the same time. Here's how it works: The participant enters the chat room, types a message on his or her computer, and sends it; and it is instantly displayed on the screens of the other users in the chat room. Admission is generally not restricted. You never know who is going to be reading your messages or responding to them, so it's best to be cautious.

**Chat room** - A "place" or page in a Web site or online service where people can chat, or "talk," with each other by typing messages. It's "real-time" communication like talking on the phone, except the "talkers" are typing text as with e-mail. E-mail, on the other hand, is delayed communication.

**Client-based filter** - A software program that you install on your own computer to block access to inappropriate material, prevent kids from accessing the internet at certain times, or to prevent kids from revealing personal information. See also "filtering software" and "blocking software."

**Cookie** - A piece of information unique to you that your browser saves and sends back to a Web server when you revisit a Web site (the Web server is the computer that "hosts" a Web site that your browser downloads or "sees"). The server "tells" your browser where to put the cookie on the server. Cookies contain information such as log-in or registration information, online "shopping cart" information (your online buying patterns in a certain retail site), user preferences, what site you came from last, etc.

**Commercial service** - General term for large online services. These services are like special clubs that require membership dues. Besides providing access to the internet, commercial services have lots of content, games, and chat rooms that are available only to members.

**Cyberspace** - A very general term used in a number of ways. "Cyberspace" can refer to the electronic areas and communities on the internet and other computer networks; the culture developing on (or across) the global network of phone wires that make up the internet; a new publishing or communications medium separate from conventional media; and a "place" separate from or in addition to physical space.

**Discussion group** - An area online focused on a specific topic where users can read and add or "post" comments ("post" in the sense of posting something on a bulletin board). You can find discussion groups, also referred to as "discussion boards," for almost any topic. See also "Newsgroups".

**Directories** - Similar to search engines, directories are indexes of Web pages organised by subject.

**Domain name** - A Web site address, usually followed by .com, .org or.co.uk. See also "URL".

**Download** - Copying data from another computer to your computer. "Download" is also used to mean viewing a Web site, or material on a Web server, with a Web browser. See also upload.

**E-mail** - Electronic Mail. A way of sending messages electronically from one computer to another. Users can send memos, letters, and other word-based messages, as well as multimedia documents. E-mailing requires having a modem, connecting a telephone line to your computer, and an e-mail address (recognisable because of the "@" symbol, such as [sales@Alphatech.com](mailto:sales@Alphatech.com)).

**Ethernet**- the most common technology for connecting computers together in a network.

**FAQ**- A list of "Frequently Asked Questions" about a specific Web site, mailing list, product, or game. Reading the FAQ first is a great idea when you are new to a site, mailing list, discussion group, or product.

**Filtered ISP** - An Internet Service Provider (ISP) that automatically blocks access to content that is inappropriate for children. Each filtered ISP uses its own company criteria to decide which Web sites are inappropriate. When choosing a filtered ISP, parents and other caretakers should make sure the company's criteria are consistent with their own values and judgments.

**Filtering software** - Software that sorts information on the internet and classifies it according to content. Some filtering software allows the user to block certain kinds of information on the internet. See also "Blocking Software," "Client-Based Filtering Software," and "Server-based Filtering Software."

**Firewall**- A security device that places a protective "wall" around a computer or network of computers, keeping it from being accessible to the public.

**FTP** - File Transfer Protocol - a way to transfer ("download" or "upload") files from one computer to another, for example from your hard drive to a Web server in order to update a Web site.

**Flaming** - Sending a nasty piece of e-mail or posting a nasty comment in a newsgroup or discussion group, usually in response to a posting that offended someone.

**Gateway** - Generally any device that provides access to another system. For example, an ISP might be called a gateway to the internet; also a hardware device that connects a local network to the internet.

**Hardware** - The nuts, bolts, and wires of a computer and computer-related equipment, also the actual computer and related machines such as scanners and printers.

**Hyperlink** - An image or portion of text on a Web page that is linked to another Web page (either on the same site or in another Web site). If it's a word or phrase, you can tell it's a link because it's another colour, it's underlined, or both. If it's an image, you can tell it's a hyperlink if you see a border around it, or if the cursor changes to a little hand when you drag the cursor over the image with the mouse. You just click on the link to go to another Web page or another place on the same page. See also links.

**HTML** - Hypertext Markup Language - The standard language used for creating documents on the World Wide Web.

**HTTP** - Hypertext Transfer Protocol - The standard language that computers connected to the World Wide Web use to communicate with each other.

**Home page** - The first page or document Web users see when connecting to a Web server or when visiting a Web site.

**ICRA** - Internet Content Rating Alliance rating system - a rating system for Web content (see also RSACi).

**IMor Instant Message** - A chat-like technology on an online service that notifies a user when a friend is online, allowing for simultaneous communication (like talking on the phone, only with text). See also "Web-based instant messaging."

**Internet**- Referred to as "Net" for short, a collection of thousands of connected computers and computer networks.

**Intranet** - A private network that works like the internet, except that it can only be seen by a select group of people, such as the employees of a company.

**IRC** - Internet Relay Chat - A part of the internet (not on the Web) that allows participants to "chat" online in a live forum that usually centers around a common interest. IRC is the earliest form of online chat.

**ISDN** - Integrated Services Digital Network - A technology that allows you to connect to the internet over standard phone lines at speeds higher than a 56k modem allows. The technology is older and the connection speed lower than those of ADSL.

**ISP** - Internet Service Provider - A company that sells access to the internet, most often through a local phone number. ISPs are usually distinguished from commercial services, which link to the internet but also offer additional services, such as content and chat, only available to their subscribers.

**IP** - Internet Protocol - The computer language that allows computer programs to communicate over the internet.

**Java** - A computer programming language that allows World Wide Web pages to have animation, calculators, and other fancy tricks. See also "applets".

**Keyword** - On Web search engines, these are words that you type into the search form, or search "window," to search the Web for pages or sites that contain your keyword and information related to it.

**LAN**- Local Area Network - A network of connected computers that are generally located near each other, such as in an office or company.

**Link** - Highlighted text that is designed so that clicking on it will take you to another document, Web page, or Web site. See also hypertext.

**Modem** - A hardware device that allows computers to communicate with each other over telephone lines. Modems come in different speeds: The higher the speed, the faster the data are transmitted. A modem enables what is generally referred to as "dial-up access." The fastest widely available modems are "56K" (or 56 kilobits per second).

**Monitoring software** - A type of software product that allows a parent or caretaker to monitor the Web sites or e-mail messages that a child visits or reads, without necessarily blocking access.

**Mouse** - A small device attached to your computer by a cord, which lets you give commands to the computer by clicking the device. See also hardware.

**Multimedia**- A combination of two or more types of information such as text, audio, video, graphics, and images.

**Netiquette** - The rules of cyberspace civility. Usually applied to the internet, where manners are enforced exclusively by fellow users.

**Newsgroups** - Discussion groups on the internet (not on the Web, which is only one area of the internet) that are broken down and categorised by subjects. These discussion groups consist of messages sent by other internet users and displayed publicly for everyone in the group (or under the topic area) to read. The word "news" in "newsgroups" does not mean they are run by news services or journalists.

**PICS** - Platform for Internet Content Selection - PICS is a technology that allows Web browsers to read content ratings of Web sites, but it is not a rating system itself.  
**Plug-in** - A program that works with browsers to play audio and video.

**Port Scanning- Port Scanning** is an activity, which by using a particular type of software gives the user the ability to scan the computer system of another internet user. The purpose of which can be (but is not limited to), passwords and usernames, remotely controlling that computer or destroying data on that computer.

**Posting** - Like posting a message on a bulletin board, the sending of a message to a discussion group or other public message area on the internet. The message itself is called a "post."

**PSTN** - Public Switched Telephone Network. A circuit-switched analogue network which makes connections for the duration of telephone call. These connections are usually used for voice but can also carry data between facsimile machines and computers (via a modem).

**RSACi** - Recreation Software Advisory Council's internet rating system - a rating system for Web content that uses PICS technology. RSACi was recently renamed the Internet Content Rating Alliance (ICRA)

**Search engine** - A tool to help people locate information available on the World Wide Web. By typing in keywords, users can find numerous Web sites that contain the information sought.

**Server** - A host computer that stores information and/or software programs and makes them available (or "serves" them) to users of other computers. You download the information on a

#### **Web server with a Web browser**

Server-based filter - Unlike client-based software, which is installed on your own computer, server-based filters work on a host server (for example, a Web server) generally located at an Internet Service Provider or a LAN at a company. Your computer is connected to this server so that you receive only the Web pages that are not filtered on the server.

**Software**- A computer program. Loosely defined, it's made up of a set of instructions, also called "computer code," to be used on your hardware. There is "system software" that operates the machine itself (such as the Windows and MacOS operating systems), and there is "application software" for specific uses, or applications, such as word processing, playing games, or managing your money.

**Spider** - A software program that "crawls" the Web, searching through Web pages and sites and indexing those pages in a database of Web pages that can then be searched using a search engine.

**Spam** - Unsolicited "junk" e-mail containing advertising or promotional messages sent to large numbers of people. Sometimes people or companies send sexually explicit unsolicited e-mail, known as "porn spam."

**TCP/IP** - Transmission Control Protocol / Internet Protocol - A computer "language" that allows for transmission, or "publishing," of information across the internet.

**Time limiting software** - Software that allows time limits to be set for access to the internet or software programs such as games.

**Trojan (Horse)** - A Trojan (horse) is an "apparently useful program containing hidden functions that can exploit the privileges of the user [running the program], with a resulting security threat. A Trojan horse does things that the program user did not intend" Trojan horses rely on users to install them, or they can be installed by intruders who have gained unauthorised access by other means. Then, an intruder attempting to subvert a system using a Trojan horse relies on other users running the Trojan horse to be successful.

**Upload** - Copying or sending data or documents from your computer to another computer, such as the server that hosts your home page. See also download.

**URL** - Uniform Resource Locator - The World Wide Web address of a site on the internet. For example, the URL for this website is <http://www.abuse-guidance.com>. See also Domain Name.

**Web** - The World Wide Web - What most people think of when they think of the internet. The

Web is actually just one service on the internet. It is a collection of graphical hyperlinked documents made publicly available on computers (or Web servers) around the world. The information on these servers can be viewed or accessed with a browser. Other services on the internet include Internet Relay Chat and Newsgroups.

**Web-based chat** - As opposed to chat IRC found on subscriber-only online services, Web-based chat allows people to chat with each other using a browser. Web-based rooms are found in Web sites.

**Web-based e-mail** - A technology that allows you to send and receive e-mail using only a browser(as opposed to an e-mail software program like Eudora).

**Web-based Instant-Messaging** - Instant-Messaging technology that works in Web sites (as opposed to a commercial online services). See also "Instant Messaging".

**Webmaster** - The administrator responsible for the management and often design of a Web site.

**WWW** - The World Wide Web. See "Web".