Acceptable Use and Fair Usage Policy

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.

Unified Business Communications (UBC) 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, UBC 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".

UBC 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. Our current terms and conditions have previously been issued to you and are deemed incorporated herein.

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

a. Common Sense

The majority of UBC 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.

b. 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.

c. Improper Use of Public Telecommunication System.

To connect to any of UBC 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.

"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".

d. 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!

e. Sharing Logon Details

UBC prohibits customers from sharing details.

f. Port Scanning

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

g. 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 (know as SPAM).

As UBC 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 UBC services.

3. **Internet Access: Acceptable Usage Policy**

a. 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.

b. 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.

c. 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 UBC with a copy of the written consent received from the target of the scan authorising the activity. This must be supplied to UBC prior to the application being run.

d. 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.

e. 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.

f. What Action Will UBC Take?

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

UBC 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 UBC's discretion, upon receipt of a written undertaking by the abuser not to commit any future "abuse". All cases are, however, considered by UBC on their individual merits.

4. 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:

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

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 (know as SPAM).

As UBC 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 UBC services.

5. Email- Acceptable Use Policy

a. Introduction

Exchanging emails with others generally involves using common sense regarding the content material and being polite and courteous. The vast majority of UBC's 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.

b. Spam

(Unsolicited Bulk emails) You must not use UBC's 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.

c. 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. UBC 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.

d. 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 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.

e. What Action Will UBC Take?
Compliance with this Acceptable Use Policy is a contractual requirement. If you fail to do so, your service may be suspended or terminated.

UBC 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 UBC's discretion, upon receipt of a written undertaking by the abuser not to commit any future "abuse". All cases are, however, considered by UBC on their individual merits.

6. 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 Messages 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 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.

7. Chat & Instant Message Service - Acceptable Use Policy a. Introduction

a. 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'.

b. 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')

c. 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.

d. What Action Will UBC 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. UBC 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 UBC's discretion, upon receipt of a written undertaking by the abuser not to commit any future 'abuse'. All cases are, however, considered by UBC on their individual merits.

8. Static Public Internet Protocol (IP) Addresses

Certain systems and applications require one or more Static Public Internet Protocol addresses to be assigned to an internet service by the ISP. With many of our internet services we can and do supply these addresses and endeavour to keep them unchanged for the lifetime of the service we provide. However in some cases it may be necessary to change the IP address associated with to the services we supply. Where possible we will notify the customer by phone or by email in advance of the change– however any charges or loss of service that may be incurred by the customer as a result of these changes will be

governed by our prevailing terms and conditions