

## **LCC xDSL 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.

LCC's 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, LCC 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".

LCC's 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 LCC's 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 LCC's 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**

LCC prohibits customers from sharing details.

### **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 LCC 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 LCC services.

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

#### **Introduction**

LCC's relationships with its customers, other networks, and ultimately its connectivity to the rest of the Internet, require its customers to behave responsibly. Accordingly, LCC cannot permit irresponsible behaviour by its customers, which could damage these relationships, LCC's 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.

#### **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 LCC with a copy of the written consent received from the target of the scan authorising the activity. This must be supplied to LCC 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.

#### **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 LCC 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 LCC 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 LCC'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.

### **Spam (Unsolicited Bulk emails)**

You must not use LCC'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.

### **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. **What Action Will LCC Take?**

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

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