Revised October 2009

Acceptable Use

Statement of 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 behaviours 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 the law.

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, ELOG has developed a number of Acceptable Usage Policies. These policies should help you benefit from safer surfing and minimise the risk of suffering "online abuse".

We have also included some general advice on how to protect you and your computer to each of these policies which we encourage you to follow.

2. ILLEGAL AND INAPPROPRIATE ACTIVITIES

As an ELOG Customer you will need to connect to the internet to receive our services. Whilst connected to the Internet and equipment operated by ELOG you must comply with the relevant laws that apply in the UK. You should also be mindful of the fact that the Internet is a global medium and is regulated by the laws of many different countries. Material which is legal in this country may be illegal in another and vice versa.

These are some of the things that you must not do whilst connected to the Internet:

You must not, by using the service, download, possess or transmit in any way, illegal material (for example indecent images of children).

You must not send, publish, distribute, circulate or otherwise propagate any material that may be deemed to be grossly offensive or of an indecent, obscene nature or menacing in character.

You must not send, with the intention of causing annoyance, inconvenience or needless anxiety a message that you know to be false, or to cause such a message to be sent or to persistently make use of our service for that purpose.

You must not gain or attempt to gain unauthorised access to any computer systems for any purpose, including accessing the Internet.

You must not, without authorisation intentionally impair or attempt to impair the operation of any computer, prevent or hinder access to any program or data held in any computer or to impair the operation of any such program or the reliability of any such data (this could include deleting files, changing the desktop settings introducing viruses etc.).

You must not infringe the rights of others, including the right of privacy and copyright (an example would be sharing without permission of the copyright owner protected material such as a music or video file).

Many of these activities could result in legal action, a fine or a term of imprisonment or both.

If you are in any doubt as to the legality of anything, take independent legal advice before proceeding.

3. ELOG'S OBLIGATIONS

ELOG is obliged under the Regulation of Investigatory Powers Act to disclose information to Law Enforcement Agencies and Public Authorities that are legally entitled to obtain such information. Similarly ELOG must comply with court orders to disclose information. In serious instances of abuse we may also notify the police or relevant law enforcement agency.

ELOG cannot and does not monitor content of its customers data or webspace or content of chat rooms, instant messaging, email, newsgroup or indeed of any communications and therefore ELOG cannot and does not guarantee that all of these are free of illegal material or other content considered unacceptable by others including the Internet community.

4. CHANGES TO THE ACCEPTABLE USE POLICIES

We may change the Acceptable Usage Policies' from time to time and will inform you on this website when we do so. 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.
Please note that our AUP's were last updated in [April 2009].

5. BREACHES OF ACCEPTABLE USE POLICIES

Reports of breaches of these acceptable use policies by ELOG customers can be sent to **abuse@elogistics.com**

ELOG may operate systems to ensure compliance with these acceptable use policies, including without limitation network scanning and testing of open servers and mail relays.

6. WEBSPACE - ACCEPTABLE USE POLICY

While webcasting using ELOG servers you must comply with the law.

You must not have illegal material on your website or host a link to material that is illegal, wherever it is hosted.

Your webspace may not be used to distribute or advertise any of the following material:

1. Software for sending unsolicited bulk emails, excessive news postings etc.
2. Software for port scanning, virus creation, hacking or any other illegal or antisocial activity.
3. Lists of email addresses except where all the addressees have given their explicit permission.
4. Any collection of personal data other than in accordance with all applicable data protection legislation.
5. Links to websites hosting illegal content.
6. Content designed to offend or cause needless anxiety to others.

Your webspace should not be used to incite disorder or publish any material which constitutes instructions to commit illegal activities.

You must not use expressions that are offensive to others on grounds of gender, race colour, religion or other similar categories.

You must not make statements that are defamatory to or misrepresent others. Defamatory postings may include but are not limited to postings which harm the personal or business reputation of another or exposes him to hatred, contempt or ridicule, or lowers him in the estimation of his community, or deters other people from associating or dealing with him.

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

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

You must ensure that your index.htm or default.htm file (the first page to be viewed on your webspace) does not contain any material liable to offend. A clearly readable warning page must be displayed before any adult material is displayed. Equally, if you have any doubt about the suitability of your content for others, in particular to minors, you must display a warning page before a visitor reaches the content. If in doubt, seek independent legal advice.

You must not share the password for your webspace. Your passwords are your responsibility and must not be disclosed to a third party.

ELOG cannot and does not 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 by the Internet community.

SOME ADVICE ON HOW TO PROTECT YOU AND YOUR COMPUTER

As part of certain Internet services, ELOG offers its customers personal webspace. This is an area on ELOG's Internet servers that you can present and display material to the World Wide Web (WWW).

Make sure you do not display too much personal detail on your webspace and remember that you publish any personal information at your own risk.

Be careful with content that may lead to argument; this is especially important if your website is also your primary email address. Not everyone will have 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.

7. EMAIL - ACCEPTABLE USE POLICY (AUP)

While connected to the Internet via ELOG servers you must comply with the law.

You must not intentionally or unwittingly participate in the sending of unsolicited email, bulk or otherwise. This applies to material which originates on your computer system as well as third party material which passes through your system, with or without your knowledge

You must not send email which has forged header information, nor should you attempt to impersonate any other individual or organisation.

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.

If you are a business user and use a mailing list to send marketing or similar correspondence it is your responsibility to keep it up to date and to ensure that all un-subscribe requests are dealt with promptly; failure to do so may result in any subsequent complaints being dealt with in the same manner as complaints of unsolicited mail, bulk or otherwise.

SOME ADVICE ON HOW TO PROTECT YOU AND YOUR COMPUTER

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

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 or cause to be sent any emails which cause annoyance, inconvenience or needless anxiety (e.g. subscribing someone to a mailing list without their authorisation). 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.

Although much unsolicited bulk 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.

Email is sometimes used as a vehicle to attempt to lure Internet users into divulging personal information via bogus emails and or websites in what are known as “phishing” attacks. Increasingly, criminals are becoming very adept at creating accurate facsimiles of official communications and websites of financial and other institutions and you should satisfy yourself that you are in receipt of genuine email from them. If you are not, you should contact the organisation by another means to validate the communication.

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.

Be 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.

Consider that if you post your email address publicly on the Internet (for example on a personal website) it may be harvested by others for the purpose of adding to spam lists.

Be wary of so-called spam email cancellation services. They might be bogus services that collect rather than block email addresses for spam lists.

When filling in on-line forms always look for and complete any “opt in” or "opt out" boxes to reflect your wishes about being contacted regarding advertisement and promotion of any products and services.

If you become a victim of abusive emails, there may be little that your Internet Service Provider (ISP) can do to stop the abuse. However, the ISP of your abuser may be able to take action under its own terms and conditions as ELOG would try to do on receipt of such a complaint. Accordingly, we recommend that you send an email to the "abuse department" of the email sender’s ISP (i.e. abuse@ the ISP) attaching the abusive email and all of its header (the full addressing) information.

It is unlikely that any ISP will provide you with the name and details of an alleged offender. However, an ISP may be obliged to divulge such information to appropriate authorities, such as the police or the courts, if formally requested to do so.

In cases of extreme 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.