

ACCEPTABLE USE POLICY

Image Telecom Solutions Ltd



Acceptable Use Policy

Issue: 1.2

Issue Date: 1 January 2007

ACCEPTABLE USE POLICY

This Acceptable Use Policy (“**AUP**”) should be read in conjunction with the Image Telecom Solutions Ltd (“**ITS**”) Terms and Conditions, which is provided to all clients when agreeing a contract for the provision of services.

The term ‘Client’ within this policy refers to the Person with whom ITS has entered into a contractual relationship. For the purposes of this document the term is equally applicable to resellers and direct clients of ITS.

The term ‘End User’ within this policy refers to the person or persons who are utilising the ITS-provided service, whether directly or indirectly as part of a solution supplied by an ITS reseller.

1. Introduction

1.1 The AUP has been designed to protect ITS, Client’s resources and peering networks in order to maintain the provision of high speed network and high availability services whilst ensuring that as an Internet Service Provider, we comply with all the relevant UK Laws.

1.2 ITS offer Clients a range of quality, competitively priced network and information technology services. It is the responsibility of our Clients to ensure that all End Users of these services comply with the latest edition of the AUP at any given time.

2. General Guidelines

2.1 Any use of the ITS network or of the Internet Services operated on or via the network, such as World Wide Web, e-mail, news, gopher or Telnet services, will be admissible solely within the framework of the applicable provisions specified by English law and within the framework of the service offering contractually agreed upon with the Client.

2.2 Specifically, this means that the ITS network must not be used for sending, receiving or distributing content that:

- (a) constitutes offences such as sedition; forbidden extremist political propaganda; invasion of personal privacy including insult, libel and defamation; or distribution of pornographic literature, or
- (b) is indecent, defamatory, obscene or menacing or otherwise offensive, or
- (c) violates a third party’s rights such as the right to bear a name, the right of personality, copyrights, competition and trademark laws. The End User must also observe the legal provisions concerning data protection and the protection of a third party’s privacy.

2.3 In addition to the above, the services operated by ITS must not be used for improper purposes.

2.4 Such improper purposes include any use that impairs the integrity and performance of the network or its parts and dial-in points to an extent exceeding what has been contractually agreed upon. Misuse also includes the use of the network for distributing, loading or publishing data that could violate or impair a third party’s rights or constitute a threat or insecurity to a third party.

2.5 It is not admissible to use the services available on or via the ITS network of obtaining data or information that is not intended for the End User. This also includes the misuse of the services for the purpose of copying, tapping or intercepting

e-mail messages or other digitally transmitted information that is not intended for the recipient.

2.6 It is not admissible to use the services for circumventing security mechanisms that protect foreign computers or computer systems, networks or network access facilities, for gaining unauthorised access to foreign computer systems (“hacking”), for performing activities in preparation for the unauthorised access to a foreign computer system (eg port scans) or for impairing the performance of a computer, computer system or network to an extent that goes beyond the services commonly rendered (“denial of service” attacks).

2.7 It is not admissible to use the services for distributing programs that serve the purpose of either causing damage to other users or computer systems (eg virus infection programs) or gaining unauthorised access to foreign computer systems (“Trojan Horses”).

2.8 ITS’ Clients are responsible for taking all reasonable measures to control traffic that is sent from their End Users connections. It is their responsibility to ensure that all software on their side of the connection is virus-free and up-to-date with all relevant security patches. In particular, server software running on public-facing ports, such as mail servers and proxy servers, must not be remotely exploitable.

2.9 If ITS find malicious traffic emanating from and End User connection, we have an obligation to our other Clients and peering networks to take urgent measures to block that traffic. In many cases, this can be achieved by selective port blocking, but in other cases, this will involve disconnecting and suspending the account until the issue has been resolved. ITS understand that in many cases, the Client may not be responsible for or aware of a problem, and will work with the Client to resolve the issue as efficiently as possible to restore normal service.

2.10 End Users may not mount an attack, by whatever means, against any of the ITS systems. End Users may not run unauthorised mailing lists from, or through any of the ITS machines, or e-mail servers.

2.11 The Internet has global reach and, although the Mater Services Agreement is governed under English law, Clients must take all reasonable steps to avoid breaching relevant foreign laws.

3. Internet Access

3.1 The use of the network circuits that provide access to the ITS network is restricted to Clients and End Users having a contractually agreed access right, which has been granted either by ITS itself or by any of its partners being authorised to grant such access rights.

- 3.2 The End User is not allowed to transfer his/her access right; neither directly nor indirectly, to any third party without ITS' express consent. This excludes persons involved in the Client's business operations or persons sharing a common household with the End User.
- 3.3 The access and authentication data that is given to the End User for access to the ITS network must be protected at all times. Passwords protecting the access to the network must be kept confidential checked and modified if unauthorised use by a third party is suspected.

4. Fair Usage Quotas

- 4.1 ITS operate a fair usage quota on specific DSL services. The Following download bandwidth allowances will apply, per End User per month, for those named services that are provisioned on 'per user' charging tariff. These monthly download quotas are only enforced where a more specific cap – whether it be higher or lower than the stated bandwidth allowance below – is not explicitly stated as part of the services being provisioned.
- ADSL Home Connections: 40GB per month
ADSL Business Connections: 100GB per month
SDSL Business Connections: 100GB per month
- 4.2 Where an End User exceeds their permitted fair usage quota, ITS reserve the right to reduce their bandwidth (typically to sub 100kb/s throughput) for the remainder of that month.

5. Electronic-mail

- 5.1 It is not admissible to distribute e-mail messages to persons not wishing to receive such messages, especially in the event that the distribution of such electronic mail is done for the purpose of confronting a single person or numerous persons with unwanted commercial advertising, political statements or announcements of any kind. The Client and End Users must refrain from sending such and similar messages to news groups; this applies in particular to the distribution of such e-mail to multiple news groups ("cross-posting"). It is also inadmissible to send multiple e-mail messages for the purpose of impairing or paralysing the recipient's e-mail or news service ("mail-bombing").
- 5.2 It is not admissible to modify or falsify the information that is contained in the header of an e-mail message or news article. Every Client and/or End User operating an e-mail service on the ITS network must ensure that his/her service cannot be used by any third party for the purpose of sending anonymous e-mail messages or distributing messages ("foreign relaying") that might offend against the guidelines specified herein.

6. Policy Changes

- 6.1 ITS reserves the right to amend this Acceptable User Policy in line with changes in the Internet Service Provider sector. New versions of the AUP will be introduced at the rate of no more than one per calendar quarter, with the most recent version always being available on the ITS website at www.image-telecom.com/downloads