

# Acceptable usage policy

## 3 Acceptable Use Policy

The term "Supplier" refers to a1isp.co.uk. The term "Customer" refers to the person, organisation, or company making an agreement for provision of services or equipment directly with the Supplier.

**3.1 Scope.** The Supplier's resources are limited, and abuse of its resources by one user can be detrimental to others. The Supplier also wishes to maintain a reputation as a reputable and responsible service provider. Using resources in a manner that is detrimental to other users or to the Supplier itself is not acceptable, and is grounds for immediate termination of service without refund. The following terms are included without limitation as examples of what should and should not be done in the spirit of acceptable use. Breach of the acceptable use policy constitutes a breach of the terms and conditions of service and allows the Supplier, at its sole discretion, to terminate the offending account without refund, whether explicitly stated or not.

**3.2 Third Party**  
Accountability. Customers will be held responsible and accountable for any activity by third parties using their account that violates guidelines created within the Acceptable Use Policy. Users are obliged to ensure that their accounts remain secure.

**3.3 Security.** Use of the Supplier's service to access, or to attempt to access, the accounts of others, to penetrate, or attempt to penetrate, security measures of the Supplier's or another entity's computer software or hardware, electronic communications system, or telecommunications system, whether or not the intrusion results in the corruption or loss of data, is expressly prohibited and the offending account is subject to immediate termination as described in section 1.5. Users are prohibited from violating or attempting to violate the security of the network. (The Supplier is under no duty to look at each Customer's or user's activities to determine if a violation of the terms and conditions has occurred, nor do we assume any responsibility through our terms and conditions to monitor or police internet related activities). Violations of system or network security may result in civil or criminal liability. The Supplier will investigate occurrences, which may involve such violations and may involve, and cooperate with, law enforcement authorities in prosecuting Users who are involved in such violations. This largely, but not exclusively includes taking any action in order to obtain services to which such User is not entitled.

**3.4 Content.** You may not use the Supplier's infrastructure, or service bought, or rented from the Supplier to publish material, which the Supplier determines, at its sole discretion, to be unlawful, indecent or objectionable. For purposes of this policy, "material" refers to all forms of communications including narrative descriptions, graphics (including photographs, illustrations, images, drawings, and logos), executable programs, video recordings, and audio recordings. If an account is used to violate the Acceptable Use Policy or our Terms and Conditions, we reserve the right to terminate your service without notice. We prefer to advise Customers of inappropriate behaviour and any necessary corrective action, however, flagrant violations of the Acceptable Use Policy will result in immediate termination of service. Our failure to enforce this policy, for whatever reason, shall not be construed as a waiver of our right to do so at any time.

**3.5 Illegal Use.** The Supplier's services may not be used for illegal purposes, or in support of illegal activities. The Supplier reserves the right to cooperate with legal authorities and/or injured third parties in the investigation of any suspected crime or civil wrongdoing.

### 3.6 Threatening

#### Behaviour. The

Supplier's services may not be used to transmit any material (by e-mail, uploading, posting or otherwise) that harasses others, or threatens, or encourages bodily harm or destruction of property.

### 3.7 Fraud,

Forgery, & Impersonation. You may not use the Supplier's service to commit, attempt to commit, or aid those attempting to commit any kind of fraudulent activity. This includes fraudulent offers to sell or buy products, items, or services, or to advance any type of financial scam such as "pyramid schemes," and "chain letters". Attempting to or adding, removing or modifying information in an attempt to mislead the recipient for example, forging packet header information to impersonate someone is forbidden.

### 3.8 "Spam" Mail. Anyone deemed by

the Supplier to be using services to send spam mail, or hosting services or features that either aid or enable others to send spam mail will have their accounts terminated immediately without refund or notice. This includes, Usenet spamming, News bombing, and message forging.

### 3.9 Copyright or

Trademark Infringement. Use of the service to transmit any material (by e-mail, uploading, posting or otherwise) that infringes any copyright, trademark, patent, trade secret or other proprietary rights of any third party, including, but not limited to, the unauthorized copying of copyrighted material, the digitization and distribution of photographs from magazines, books, or other copyrighted sources, and the unauthorized transmittal of copyrighted software.

### 3.10 Collection

of Personal Data. Use of the service to collect, or attempt to collect, personal information about third parties without their knowledge and consent.

### 3.11 Malicious

and Unfriendly Activity. Supplier's services may not be used for any activity which affects the ability of other people or systems to use network or the Internet. Interference with or disruption of other network users, services or equipment is prohibited. It is the Customer's responsibility to ensure that their network is configured in a secure manner. A Customer may not, through action, omission of action, or inaction, allow others to use their network for illegal or inappropriate actions. A Customer may not permit their network, through action or inaction, to be configured in such a way that gives a third party the capability to use their network in an illegal or inappropriate manner. Intentional distributions of software or "viruses" that attempt to and/or cause damage, harassment, or annoyance to persons, data, and/or computer systems are prohibited.