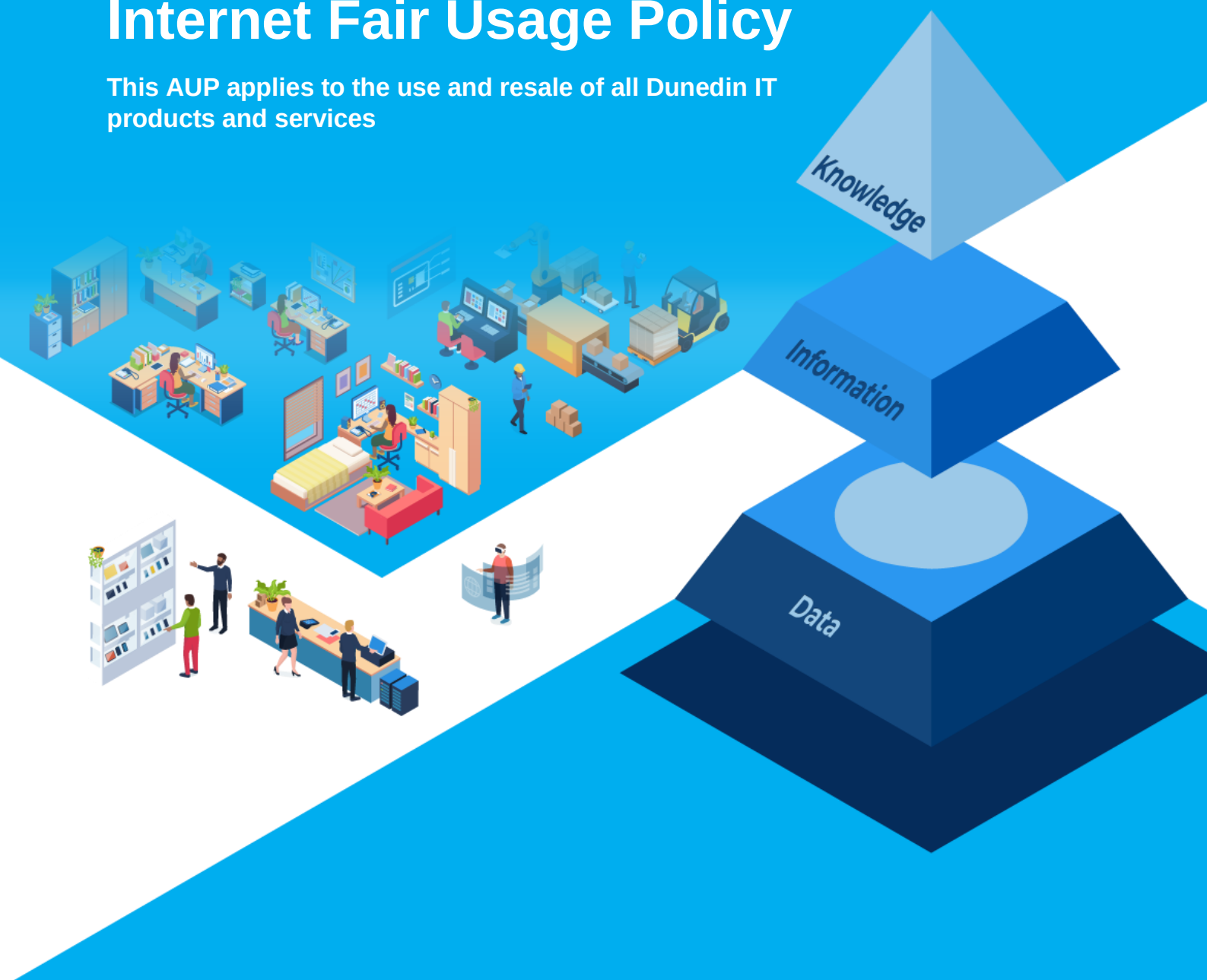
Version: 1.1
Issued:

Internet Fair Usage Policy

This AUP applies to the use and resale of all Dunedin IT products and services



Version: 1.1 Issued: 18 May 2020

Introduction

Dunedin IT operates a high capacity network and we expect the end users of our networks want to enjoy the benefits of gigabit Internet and dark fibre.

Where a product is advertised as unlimited, it does not have any data caps or any artificial speed restrictions. There are however some restrictions in how the services we provide can be onward used. These relate to our relevant legal and contractual obligations, a summary of which is below.

We don't want to list lots of things you can and cannot do but ask that you agree not to misuse the service. This includes but is not limited to using the services for purposes that are illegal, improper, infringe the rights of others, or adversely impact others' enjoyment of the services.

Examples of inappropriate use

The list below is informed by relevant legislation, including the Telecommunications Act 1984, the Computer Misuse Act 1990 and the Regulation of Investigatory Powers Act 2000 (as updated from time to time).

- 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 by us to be grossly offensive, of an indecent, obscene nature or menacing in character (for example, libel, slander, invasion of privacy, harassment, obscenity, etc.).
- You must not send, with the intention of causing annoyance, inconvenience or needless anxiety a message that you know to be false or cause such a message to be sent.
- You must not use the service to interfere or attempt to interfere with the operation of Dunedin IT's equipment or services or the Internet, or to interfere or attempt to interfere with other people's enjoyment of the Internet or their systems or equipment.
- You may not access or modify any computer material without authorisation.
- You must not infringe the rights of others, including the right of privacy and copyright (an example would be sharing protected material, such as a music or video file, without permission of the copyright owner).
- If you are using our service to carry voice traffic you must comply with the relevant OFCOM regulations relating to nuisance and other calls.

This Policy prohibits the following:

- **Impersonation/Forgery**

Adding, removing, or modifying identifying network header information ("spoofing") in an effort to deceive or mislead is prohibited. Attempting to impersonate any person by using forged headers or other identifying information is prohibited. The use of anonymous re-mailers and nicknames does not constitute impersonation. Using deliberately misleading headers ("munging" headers) in news postings in order to avoid spam e-mail address collectors is allowed provided appropriate contact information is contained in the body of the posting.

- **Privacy Violations**

Attempts, whether successful or unsuccessful, to gain access to any electronic systems, networks or data, without proper consent, are prohibited.

- **Threats**

Threats of bodily harm or destruction of property are prohibited.

- **Harassment**

Threatening or harassing activity is prohibited.

- **Illegal Use**

The use of this service for illegal purposes is prohibited.

- **Reselling**

The resale of any service without our proper authorisation is prohibited.

- **Copyright Infringement**

All material published must be owned by the publisher or the appropriate releases must have been obtained prior to publishing. Dunedin IT will co-operate with all agencies attempting to assert their rights in these matters.

Network Disruptions and Network-Unfriendly Activity

Any activities, which adversely affect the ability of other people or systems to use Dunedin IT services or the Internet, are prohibited. This includes "denial of service" (DoS) attacks against another network host or individual user.

Interference with, or disruption of, use of the network by others, network services or network 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 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 it gives a third party the capability to use their network in an illegal or inappropriate manner.

E-Mail

Dunedin IT does not tolerate, endorse or participate in e-mail spamming. Sending unsolicited commercial e-mail is prohibited. We cannot authorise bulk e-mailing although we do recognise that in some instances this is a valid and useful form of marketing for both senders and recipients.

Sending large volumes of unsolicited e-mail, whether or not that e-mail is commercial in nature is prohibited. All solicited e-mail should have been confirmed through the use of a double opt-in list (i.e. the recipient must confirm their wish to receive that particular e-mail twice).

Activities that have the effect of facilitating unsolicited commercial e-mail, or large volumes of unsolicited e-mail, whether or not that e-mail is commercial in nature, are prohibited. Users operating mail servers must ensure that they are not open relays.

Anonymous bulk e-mailings are not permitted, and we will terminate the accounts of any customers who attempt to do this. This may happen without notice.

If we receive any complaints from recipients or other third parties, or any mailing causes technical problems on our systems, we may take further action to stop this happening again. This may involve the termination of any accounts the sender has and may occur without notice.

In the event that we are alerted to anyone sending bulk e-mails, we will generally attempt to make contact with the senders to discuss appropriate actions.

Senders must give recipients the ability to easily contact the sender and remove themselves from their mailing list.

Senders must be sure that recipients are aware that they are listed on the sender's emailing list and that they themselves provided their information or authorised a third party to do so on their behalf.

In the event of any problems being caused by this type of activity, we will make every effort to ensure that the problem is resolved as quickly as possible. This includes full co-operation with any relevant authorities.

Facilitating a Violation of this AUP

Advertising, transmitting, or otherwise making available any software, program, product, or service that is designed to violate this AUP, or the AUP of any other Internet Service Provider, which includes, but is not limited to, the facilitation of the means to spam.

The list above is illustrative and by no means exhaustive. Inappropriate use could result in legal action, a fine or term of imprisonment or both.

Your responsibilities

The Internet and telecommunications in general are subject to on-going change. As the law evolves, our restrictions will follow. Regardless of changes to our own policy however, the following apply:

- It is always your responsibility to ensure that you're aware of the relevant legal restrictions.
- You must comply at all times with the current legislation and regulation that is in force and with the formal terms of our supply contracts.
- You are ultimately responsible and liable for your own use of the Services and for your end customers' use of the Services. We therefore advise that, where our services are resold (whether that is to other providers or to end customers), our acceptable use policy is reflected in your own onward contracts and policies.
- You are responsible for ensuring that security information (including but not limited to any usernames and passwords) remains confidential so that the services cannot be used by any unauthorised person.
- You must provide Dunedin IT with all reasonable assistance and any resources required to comply with any legal processes or requirements arising as a result of such use.

Procedures related to acceptable use

Unless required to do so by law, Dunedin IT does not regulate, control or filter the Internet or your use of the Services. We do however reserve the right to filter some traffic, for example, to stop a DDOS attack.

In the event that we receive a complaint about your use of the Internet through a formal process (e.g. a Court Order) we will follow the appropriate legal steps.

We may take action if required to by suitable Internet regulation such as the Regulation of Investigatory Powers Act 2000 (as amended).

We will comply with any court order issued to us asking for access to our network.

Contractual considerations

This Acceptable Use Policy is reflected in our contracts with our partners. In the event of a conflict between the two, the contract applies over and above this policy.

Evidence of inappropriate use may result in offending services being restricted or suspended as required by law.

Reporting to the Abuse Department

Dunedin IT requests that anyone who believes that there is a violation of this AUP should direct the information to our support staff at this address: helpdesk@dunedinit.co.uk

Customers who wish to report ‘spam’ from a non-Dunedin IT source should send copies of the e-mail they received along with full header information. Some messages may not receive a response, but Dunedin IT may use the information received at this address to aid in the development of Dunedin IT's filter lists.

All issues involving other e-mail abuse originating from Dunedin IT e-mail or network addresses should also be sent to the above address.

All issues regarding USENET ‘news’ abuse issues originating from Dunedin IT customers.

Other suspicious activity such as port scans or attempts to penetrate network resources and virus distribution.

Copyright Infringement.

Dunedin IT may take any one or more of the following actions in response to complaints:

- Issue warnings: written or verbal
- Suspend the customer's newsgroup posting privileges Suspend the customer's account
- Terminate the customer's account
- Invoice the customer for administrative costs and/or reactivation charges

What information should be submitted?

1. The IP address used to commit the alleged violation
2. The date and time of the alleged violation, including the time zone or offset from GMT
3. Evidence of the alleged violation

Copies of e-mail with full header information provide all the required information, as do syslog files and firewall logs. Other situations will require different methods.