Internet Acceptable Use Policy

This Acceptable Use Policy sets out the terms between you and us under which you may use our Internet related services ("the Services") and/or access our website at www.1-Fix.com ("our site"). This Acceptable Use Policy applies to all users of our Services and to all users of, and visitors to, our site. Use of our site is also governed by our Privacy Policy and Cookie Policy.

Your use of our Services and/or our site means that you accept, and agree to abide by, all the policies in this Acceptable Use Policy, which supplement our standard Terms and Conditions.

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 contained within this document or the 1-Fix terms and conditions. Customers must ensure that they know what these requirements are and how they are affected by them.

To enable customers to have a better understanding of what is and is not acceptable when using the internet 1-Fix has developed this Acceptable Use Policy (AUP) relating to internet services. Complying with this AUP, which is a contractual requirement, will help you benefit from safer use of the Internet and minimise the risk of suffering online abuse.

The AUP is based on current best internet industry practice and draws on the collective experience of users and service providers across the internet community. We may change this AUP from time to time.

Avoiding abuse while connected to the internet

Common sense - The majority of customers will be using commercial software to connect to and navigate the Internet. This software controls the technical aspects of the connection but there are also some simple common-sense checks, which all customers can implement. 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 the UK, for example, you should not access sites carrying child sexual exploitation and abuse material or incitement to violence.

These are just two 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 take independent legal advice.

To connect to many online services, you will use a broadband or connectivity service (SoADSL, SoGEA, FTTP or Ethernet Fibre). While connected to the internet, you must comply with legal requirements concerning telephone network use and misuse. Misuse of public electronic communications networks may constitute a criminal offence and may result in civil or criminal liability.

Use of Public Electronic Communications Network (PECN)

You must not use the Services in any way that breaches applicable law, including laws relating to unlawful, harmful, fraudulent, abusive, obscene, indecent, menacing, harassing, malicious or grossly offensive communications.

Practical steps to take

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. Malicious actors may attempt to gain unauthorised access to systems, steal credentials, disrupt services, or damage networks.
- If you keep sensitive information on your computer, it is recommended to use encryption software to protect it.
- Never install software of unknown origin. Most computer viruses and Trojans are installed unknowingly by clicking on links in email or while installing shareware or freeware applications.

Sharing log-on details

Never share log-on details.

Network misuse, security abuse and unlawful activity

1-Fix prohibits customer or third-party use of port scanning software on networks. This includes prohibitions covering:

- vulnerability scanning without permission;
- denial-of-service attacks;

- unauthorised access attempts;
- malware, botnets and command-and-control traffic;
- phishing, spoofing and credential harvesting;
- spam, mail bombing and open relays;
- infringing copyright, trade marks, database rights, confidentiality rights or other intellectual property or proprietary rights.
- hosting or transmitting unlawful content;
- excessive or abnormal use affecting network stability.

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).

1-Fix may investigate, restrict, suspend or terminate services where there is suspected abuse, security risk, legal requirement, regulator/law-enforcement request, or risk to the network.

You must notify 1-Fix promptly if you become aware of any misuse, compromise, spam, malware, credential compromise, unauthorised access or unauthorised use of your service.