Acceptable Use Policy

This Acceptable Use Policy (AUP) lists the specific actions that are prohibited when using this service and applies to all customers of our wireless internet services. This Acceptable Use Policy was formulated with the goal of enhancing the use of the Internet by preventing unacceptable use. The use of our wireless internet services constitutes acceptance of and agreement to abide by all of the policies set forth in this Acceptable Use Policy, which are in addition to and supplement the Terms & Conditions of use set out by the business provider.

We do not monitor the integrity, accuracy or the quality of the information transmitted via the service and assume no liability to its subscribers or to any third parties for the content of such information. However, we may cooperate with legal authorities and/or third parties in the investigation of any suspected or alleged crime or civil wrong doing.

By agreeing to the AUP, you are bound by the following terms & conditions:

Any breach of this Acceptable Use Policy may result in immediate suspension and/or termination of the Services.

As a subscriber or user, you hereby agree that you will not use the services for illegal purposes or to further illegal activities.

As clarification and not a limitation of the foregoing, you agree that you will not upload, download, post, distribute or facilitate the distribution of any material in any chat room, message board, newsgroup or similar interactive medium that you can access through the Services that;

- Constitutes an unauthorized reproduction of copyrighted or other protected materials or content;
- Contravenes English control laws; or
- Is threatening, abusive, harassing, defamatory, libelous, deceptive, fraudulent, or invasive of another's privacy;
- Is harmful to minors;
- Is construed to be harassing to others

Furthermore, you will not be permitted;

- To access hosts or networks without the explicit authorisation of the administration of those systems.
- To resell these services without authorisation.
- To collect personal data about a third party without their knowledge or consent.
- To breach the security of a host, network component, or authentication system without the explicit permission of the administration of those systems.
- To host any website dedicated to the sale or dissemination of pornographic materials or content and/or containing content of a sexually explicit nature.
- To monitor data on any network or system without the explicit authorization of the administration of that system or network.

- To interfere with the service of any user, host or network, including deliberate attempts to overload a server, network connected device, or network component.
- To originate malformed data or network traffic that results in damage to, or disruption of, a service or network connected device.
- To forge data with the intent to misrepresent the origination user or source.
- To send unsolicited, mass electronic mail messages to one or more recipients or systems (known as 'Spamming').
- To forge electronic mail headers (including any portion of the IP packet header and/or electronic mail address), or any other method used to forge, disguise, or conceal the user's identity when using the services ('Spoofing').

Responsibility for Your Access Code and/or Log On Details

The person’s details that are stored against a specific Access Code is responsible for the actions of any person that you allow to access this service. Each user of the network must have an individual Access Code with which to record their details against. Ultimately, any breach of the UAP will result in the named user associated with the Access Code to bear the consequences.

Network Security

Violations of network security are prohibited and may result in criminal and/or civil prosecution. We will co-operate with law enforcement authorities if a criminal violation is suspected. Examples of system or network security violations include, but are not limited to:

- Unauthorised access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of a network or to breach security or authentication measures without express authorisation of the owner of the network.

Interference with service to any user, host or network including, but not limited to:

- Mail-bombing, Packet flooding, Deliberate attempts to overload a system, Broadcast attacks, Forging of any TCP-IP packet header or any part of the header information in an email or a newsgroup posting, Unauthorised monitoring of data and / or traffic on any network or system without the express authorisation of the owner of the system or network.

Retention of user and browsing information

Publically available internet services must comply with The Data Retention (EC Directive) Regulations 2009, which forms part of the AntiTerrorism, Crime & Security Act 2001. All public internet providers have to comply with this law.

The information stored by the provider in relation to this regulation is Name, Address, Session Times and IP Address of sites visited. The information retained must be stored for a period of 12 months.

The information you provide in relation to this regulation will be held securely. This specific information will not be used by Infinium or Infinium customers using our service for any other purpose than to comply with this regulation and provide support. We will only make this information available to the relevant authorities upon a formal request to do so. Specific information provided and retained in relation to the regulatory requirements will not be used for marketing purposes.

Infinium reserves the right to revise or amend the AUP at any given time.