

# Acceptable Use Policy ("AUP")

## General

Microtalk Europe provides various internet enabled products and services including broadband, email, web hosting, voice and data services (referred to in this document as the "Services").

This document defines the Acceptable Use of the Services with a view to ensuring the integrity, security, reliability and privacy of Microtalk Europe and its suppliers networks, systems, products, services, server hosting facilities and data contained therein (collectively, the "Microtalk Europe Network").

Microtalk Europe's customers are solely responsible for the content and messages that they post, distribute or otherwise make available using Microtalk Europe's Network and Services.

Microtalk Europe encourages the use of website rating systems such as the Internet Content Rating Association (ICRA) [www.icra.org](http://www.icra.org)

For the purposes of this policy, a Customer is defined as any party who purchases a Service from Microtalk Europe.

## Illegal Use

The Microtalk Europe network may be used only for lawful purposes. Transmission, distribution or storage of any material in violation of any applicable law or regulation is prohibited. This includes, without limitation, material protected by copyright, trademark, patent, trade secret or other intellectual property rights used without proper authorisation, and material that is obscene, defamatory, constitutes an illegal threat, or violates export control laws.

## Prohibited Activities

It is contrary to Microtalk Europe policy for any of its Customers or other Service user to effect or participate in any of the activities listed below (whether actual or attempted and whether directly or indirectly) through a Service.

Each of the below practices (each, a "Prohibited Activity") constitutes abuse of Microtalk Europe's Services, Network and facilities and interferes with other Service users. Accordingly, these practices are prohibited.

1. Attempts to circumvent User authentication or security of any host, network, or account (referred to as "cracking" or "hacking"), or to interfere with the Service to any User, host, or network (referred to as "denial of service attacks"), or to deface web pages or attempt unauthorised system penetrations.;
2. Sending unsolicited commercial messages or communications in any form ("SPAM");

3. Posting or sending messages of substantially similar content to 10 or more Usenet or other newsgroups, forums, or other similar groups or lists;
4. Falsifying user or other Service related information, including, but not limited to, intentionally omitting, deleting, forging or misrepresenting transmission information, including headers, return mailing and Internet protocol addresses, provided to Microtalk Europe or to other Service users or engaging in any activities or actions intended to withhold or mask Customer's or its End Users identity or contact information;
5. Engaging in any other activity that:
  - i. threatens the integrity and/or security of any network or computer system (including, but not limited to, transmission of worms, viruses and other malicious codes and accessing any device or data without proper authorisation);
  - ii. otherwise degrades or interferes with other users' use of a Service;
6. Engaging in any of the activities listed above by using another provider's service, but channelling the activity through a Microtalk Europe account, remailer, or otherwise through a Service.

ANY INDIRECT OR ATTEMPTED VIOLATION OF THIS POLICY BY OR ON BEHALF OF A CUSTOMER OR A CUSTOMER'S END USER, AND ANY ACTUAL OR ATTEMPTED VIOLATION BY A THIRD PARTY ON BEHALF OF A CUSTOMER OR A CUSTOMER'S END USER, SHALL BE CONSIDERED A VIOLATION OF THE POLICY BY SUCH CUSTOMER OR CUSTOMER'S END USER.

## **Rights and Remedies**

Microtalk Europe may suspend and/or terminate a Customer's Service at any time for any material failure) of Customer, its representatives or its users to comply with this policy or for engaging (or permitting others to engage) in a Prohibited Activity (as determined by Ring Telecom, in its reasonable discretion.

Microtalk Europe may deny all traffic from known IP address blocks that support indiscriminate port scanning programs, or other unlawful activity, for the purpose of preserving Customer's system and network resources. Microtalk Europe reserves the right to implement technical mechanisms to prevent a Prohibited Activity