



## **INTRODUCTION**

This Acceptable and Fair Usage Policy ("AFUP") sets forth the principles that govern the use by customers of the broadband wireless network provided by iBurst (Proprietary) Limited (hereinafter "iBurst"). This AFUP is designed to help protect our customers, and the Internet community, from irresponsible, abusive or illegal activities and to provide the best mobile broadband service (the "Service") possible.

## **APPLICABLE DOCUMENTATION**

iBurst reserves the right to revise, amend or modify this AFUP from time to time without notice by posting a new version of this document on the iBurst Web site at <http://www.iburst.co.za> (or any successor URL(s)). All revised copies of the AFUP are effective immediately upon posting and supercede previous versions. Accordingly, customers and users of the Service should regularly visit our web site and review this AFUP to ensure that their activities conform to the most recent version of AFUP documentation. In the event of a conflict between any subscriber or customer agreement and this AFUP, the terms of this AFUP will govern. It is the responsibility of all iBurst mobile broadband Internet customers ("customer," "you," or "your"), and all others who have access to iBurst' network to comply with this AFUP and all iBurst policies. Additionally, it is the responsibility customers of iBurst to secure their computer equipment so that it is not vulnerable to external threats such as viruses, spam, and other methods of intrusion. Failure to comply with these or any other iBurst policies could result in the suspension or termination of the Service. If you do not agree to comply with all of these policies including the AFUP, you must immediately stop use of the Service and notify iBurst so that your account may be closed. iBurst reserves the right to terminate the Service and the Subscriber Agreement immediately if you engage in any of the prohibited activities listed in this AFUP or if you use the iBurst Equipment or Service in any way contrary to iBurst policies. You must strictly adhere to any policy set forth by another service provider accessed through the Service.

## **PROHIBITED USES AND ACTIVITIES**

Prohibited uses include, but are not limited to, using the Service, Customer Equipment, or the iBurst Equipment to:

- i. undertake or accomplish any illegal or unlawful activity. This includes, but is not limited to, posting, storing, transmitting or disseminating information, data or material which is libellous, obscene, discriminatory, unlawful, threatening, defamatory, or which infringes the intellectual property rights of any person or entity, or which in any way constitutes or encourages conduct that would constitute a criminal offence, give rise to civil liability, or otherwise violate any local or international law, order or regulation;
- ii. post, store, send, transmit, or disseminate any information or material which a reasonable person could deem to be objectionable, offensive, indecent, pornographic, harassing, threatening, embarrassing, distressing, vulgar, hateful, racially or ethnically offensive, or otherwise inappropriate, regardless of whether this material or its dissemination is unlawful;
- iii. attempt to gain unauthorized access to any other person's computer or computer system, software, or data without their knowledge and consent; breach the security of another user; or attempt to circumvent the user authentication or security of any host, network, or account. This includes, but is not limited to, accessing data not intended for you, logging into or making use of a server or account you are not expressly authorised to access, or probing the security of other hosts, networks, or accounts;
- iv. use or distribute tools designed or used for compromising or circumventing security, such as but not limited to password guessing programs, decoders, password gatherers, analyzers, cracking tools, packet sniffers, encryption circumvention devices, or Trojan Horse programs. Network probing or port scanning tools are only permitted when used in conjunction with a residential home network, or if explicitly authorised by the destination host and/or network. Unauthorised port scanning, for any reason, is strictly prohibited;
- v. upload, post, publish, transmit, reproduce, create derivative works of, or distribute in any way information, software or other material obtained through the Service or otherwise that is protected by copyright or other proprietary right, without obtaining permission of the owner;
- vi. copy, distribute, or sublicense any software provided in connection with the Service by iBurst or any third party;
- vii. restrict, inhibit, or otherwise interfere with the ability of any other person, regardless of intent, purpose or knowledge, to use or enjoy the Service, including, without limitation, posting or transmitting any information or software which contains a worm, virus, or other harmful feature, or generating levels of traffic sufficient to impede others' ability to send or retrieve information;
- viii. restrict, inhibit, interfere with, or otherwise disrupt or cause a performance degradation, regardless of intent, purpose or knowledge, to the Service or any iBurst (or iBurst supplier) host, server, backbone network, base station, node or service, or otherwise cause a performance degradation to any iBurst (or iBurst supplier) facilities used to deliver the Service;
- ix. use the iBurst network in a manner that exceeds the then current bandwidth, data storage or other limitations on the iBurst Service; or puts an excessive burden on the limitations of the iBurst network; The Subscriber acknowledges that the limitations applicable to usage of the Service are as follows:
  - ix: (a) 26 giga bytes in respect of the 64 kbps (kilo bits per second) service
  - (b) 52 giga bytes in respect of the 128 kbps (kilo bits per second) service

This is calculated based upon the theoretical max throughput of the service using a single modem, multiple modems can be used but the limitation aforementioned still applies. Once the aforementioned limitation has been reached, the Subscriber will only have access to email and voice services.

x.connect multiple computers behind the user terminal to set up a LAN (Local Area Network) that in any manner would result in a violation of the terms of this AFUP;

xi.transmit unsolicited bulk or commercial messages or "spam." This includes, but is not limited to, unsolicited advertising, promotional materials or other solicitation material, bulk mailing of commercial advertising, chain mail, informational announcements, charity requests, and petitions for signatures;

xii.transmit messages that contain threatening, abusive, illegal or libellous material;

xiii.send numerous copies of the same or substantially similar messages, empty messages, or messages which contain no substantive content, or send very large messages or files to a recipient that disrupts a server, account, newsgroup, or chat service;

xiv.distribute programs that remove locks or time-outs built into software (cracks);

xv.initiate, perpetuate, or in any way participate in any pyramid or other illegal soliciting scheme;

xvi.participate in the collection of e-mail addresses, screen names, or other identifiers of others (without their prior consent), a practice sometimes known as spidering or harvesting, or participate in the use of software (including "spyware") designed to facilitate this activity;

xvii.collect responses from unsolicited messages;

xviii.impersonate any person or entity, engage in sender address falsification, forge anyone else's digital or manual signature, or perform any other similar fraudulent activity;

xix.service, alter, modify, or tamper with the iBurst Equipment or Service or permit any other person to do the same who is not authorised by iBurst;

xx.collect, or attempt to collect, personal information about third parties without consent;

xxi.interfere with computer networking or telecommunications service to any user, host or network, including, without limitation, denial of service attacks, flooding of a network, overloading a service, improper seizing and abuse of operator privileges and attempts to "crash" a host; and

xxii.violate the rules, regulations, or policies applicable to any network, server, computer database, or Web site that you access.

## **SECURITY**

You are responsible for any misuse of the Service, even if the misuse was committed by a friend, family member, or guest with access to your Service account. Therefore, you must take steps to ensure that others do not use your account to gain unauthorised access to the Service by, for example, strictly maintaining the confidentiality of your username and password. In all cases, you are solely responsible for the security of any device you choose to connect to the Service, including any data stored or shared on that device. iBurst recommends against enabling file or printer sharing of any sort unless you do so in strict compliance with all security recommendations and features provided by iBurst and the manufacturer of the applicable file or printer sharing devices. Any files or devices you choose to make available for shared access on a home LAN, for example, should be protected with a strong password or as otherwise appropriate.

### **Security of iBurst Network and Systems**

Where all references to systems and networks under this section includes the Internet (and all those systems and/or networks to which user is granted access through of iBurst) and includes but is not limited to the infrastructure of iBurst itself.

The user may not circumvent user authentication or security of any host, device, network, or account (referred to as "cracking" or "hacking"), nor interfere with service to any user, host, device, or network (referred to as "denial of service attacks"). The host, device, network or account shall also not be used for any illegal purpose, including phishing.

Where it is found that that is a violation of the iBurst system or network security by the user are prohibited, and may result in civil or criminal liability. iBurst reserves the right to investigate incidents involving such violations and will involve and co-operate with law enforcement officials of the South African Police Services or any other Law Enforcement officials worldwide if a criminal violation is suspected. Examples of system or network security violations include, without limitation, the following:

Unauthorized access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of any system or network or to breach security or authentication measures without the express authorization of iBurst.

Unauthorized monitoring of data or traffic on the network or systems without express authorization of iBurst

Interference with service to any user, device, host or network including, without limitation, mail bombing, flooding, deliberate attempts to overload a system and broadcast attacks.

Forging of any TCP-IP packet header (spoofing) or any part of the header information in an email or a newsgroup posting.

### **INAPPROPRIATE CONTENT AND TRANSMISSIONS**

iBurst reserves the right to refuse to transmit or post and to remove or block any information or materials, in whole or in part, that it, in its sole discretion, deems to be offensive, indecent, or otherwise inappropriate, regardless of whether this material or its dissemination is unlawful. Neither iBurst nor any of its affiliates, suppliers, or agents have any obligation to monitor transmissions or postings (including, but not limited to, e-mail, newsgroup, and instant message transmissions as well as materials available on the Personal Web Pages and Online Storage features) made on the Service. However, iBurst and its affiliates, suppliers, and agents have the right to monitor these transmissions and postings from time to time for violations of this AFUP and to disclose, block, or remove them in accordance with the Subscriber Agreement and any other applicable agreements and policies.

### **ELECTRONIC MAIL**

The Service may not be used to send unsolicited bulk or commercial messages and may not be used to collect responses from unsolicited e-mail sent from accounts on other Internet hosts or e-mail services that violate this AFUP. Moreover, unsolicited e-mail may not direct the recipient to any Web site or other resource that uses the

Service. Activities that have the effect of facilitating unsolicited commercial e-mail or unsolicited bulk e-mail, whether or not the e-mail is commercial in nature, are prohibited. Forging, altering, or removing electronic mail headers is prohibited. You may not reference iBurst or the iBurst network (e.g. by including "Organisation: iBurst" in the header or by listing an IP address that belongs to iBurst or the iBurst network) in any unsolicited e-mail even if that e-mail is not sent through the iBurst network or Service. Maintaining of mailing lists by users of iBurst is only accepted with the permission and approval of the list members, and at the members' sole discretion. Should mailing lists contain invalid or undeliverable addresses or addresses of unwilling recipients those addresses must be promptly removed. Users may not forward or propagate chain letters nor malicious e-mail. Public relay occurs when a mail server is accessed by a third party and utilised to deliver mails, without the authority or consent of the owner of the mail-server. Users' mail servers must be secure against public relay as a protection to both themselves and the Internet at large. Mail servers that are unsecured against public relay often become abused by unscrupulous operators for spam delivery and upon detection such delivery must be disallowed. iBurst reserves the right to examine users' mail servers to confirm that their server is not a public relay and the results of such checks can be made available to the user. iBurst also reserves the right to examine the mail servers of any users using iBurst mail servers for "smart hosting", content filtering or similar services at any time to ensure that the servers are properly secured against public relay. All relay checks will be done in strict accordance with iBurst policy of preserving customer privacy. iBurst is not responsible for forwarding e-mail sent to any account that has been suspended or terminated. This e-mail will be returned to the sender, ignored, deleted, or stored temporarily at iBurst' sole discretion. In the event that iBurst believes in its sole discretion that any subscriber name, account name, or e-mail address (collectively, an "identifier") on the Service may be used for, or is being used for, any misleading, fraudulent, or other improper or illegal purpose, iBurst (i) reserves the right to block access to and prevent the use of any such identifier and (ii) may at any time require any customer to change his or her identifier. In addition, iBurst may at any time reserve any identifiers on the Service for iBurst' own purposes.

## **NEWSGROUPS**

Messages posted to newsgroups must comply with the written charters or Frequently Asked Questions ("FAQs") for those newsgroups as well as any other terms and conditions applicable to any particular newsgroups or provider of newsgroups. Advertisements, solicitations, or other commercial messages should be posted only in those newsgroups whose charters or FAQs explicitly permit them. You are responsible for determining the policies of a given newsgroup before posting to it. iBurst reserves the right to discontinue access to any newsgroup at any time for any reason.

The Subscriber acknowledges that excessive cross-posting (i.e., posting the same article to a large numbers of newsgroups) Posting of irrelevant (off-topic) material to newsgroups (also known as USENET spam) and related unwanted communication in this platform are all forbidden.

## **INSTANT MESSAGES**

Users alone are responsible for the contents of their instant messages and the consequences of any instant messages. iBurst assumes no responsibility for the timeliness, mis-delivery, deletion or failure to store instant messages.

## **NETWORK, BANDWIDTH, DATA STORAGE UNCAPPED RULES AND OTHER LIMITATIONS**

You must comply with all current bandwidth, data storage, and other limitations on the Service established by iBurst and its suppliers. In addition, you may only access and use the Service with a dynamic Internet Protocol ("IP") address that adheres to the dynamic host configuration protocol ("DHCP"). You may not access or use the Service with a static IP address or using any protocol other than DHCP unless you are subject to a Service plan that expressly permits otherwise. You must ensure that your activity (including, but not limited to, use made by you or others of any Personal Web Features) does not improperly restrict, inhibit, or degrade any other user's use of the Service, nor represent (in the sole judgment of iBurst) an unusually large burden on the network. In addition, you must ensure that your activities do not improperly restrict, inhibit, disrupt, degrade or impede iBurst' ability to deliver the Service and monitor the Service, backbone, network nodes, and/or other network Services. Notwithstanding that you can potentially use multiple devices; You acknowledge that iBurst's services have a limit on capacity determined by the maximum possible download capacity of a single device.

## **UNCAPPED RULES**

1. The Subscriber acknowledges that iBurst is unable to exercise control over the data passing over the infrastructure and the Internet, including but not limited to any websites, electronic mail transmissions, news groups or other material created or accessible over its infrastructure. Therefore, iBurst is not responsible for data transmitted over its infrastructure but may terminate the services:

Where iBurst infrastructure may be used to link into other networks worldwide/locally and the user agrees to conform to the Terms and conditions of their acceptable user policies (AUP) of these networks.

Where the users of the iBurst network includes not only the Subscribers of iBurst, but in the case of Resellers and Service Providers (SP's) of iBurst services, the customers/clients of the Resellers, Resellers or SP's of iBurst services are responsible for the activities of their customers/client base.

Where the Subscriber may obtain and download any materials marked as available for download off the Internet, but is not permitted/restricted to use their Internet access to distribute/copy any copyrighted materials unless permission for such distribution/copy is granted to the user by the legal owner of the materials iBurst may terminate the service immediate and without any penalty or liability.

Where the user is prohibited from obtaining, disseminating or facilitating over iBurst network any unlawful materials, including but not limited to:

- o Copying or dealing in intellectual property without authorization,
- o Child pornography, and/or
- o Any unlawful hate-speech materials.

iBurst may terminate the service immediately and without any penalty or liability.

Where iBurst needs to ensure that all Subscribers have fair and equal use of the services offered by iBurst and to protect the integrity of its network, iBurst reserves the right, and will take necessary steps, to prevent improper or excessive usage thereof. The action that iBurst may take includes, but is not limited to:

- Limiting throughput;
- Preventing or limiting service through specific ports or communication protocols; and/or
- Complete termination of service to Subscribers who grossly abuse the network through improper or excessive usage.

This policy applies to and will be enforced for intended and unintended (e.g., viruses, worms, malicious code, or otherwise unknown causes) prohibited usage.

Where online activity will be subject to the available bandwidth, data storage and other limitations of the services provided, iBurst may/can, from time to time, revise its policy and at its own discretion and provide a proper notice to the Subscribers. The Subscriber acknowledges that the limitations applicable to usage of the Service are as follows:

- 1 Gigabytes (GB) per day in Respect of the 256kbps (Kilo Bytes per second) service  
Product : iBurst Uncapped Business
- 3 Gigabytes (GB) per day in Respect of the 384kbps (Kilo Bytes per second) service  
Product: ADSL Uncapped Home. Excluding Telkom ADSL line
- 1 Gigabytes (GB) per day in Respect of the 256kbps (Kilo Bytes per second) service  
Product: ADSL Uncapped Business. Excluding Telkom ADSL line
- 3 Gigabytes (GB) per day in Respect of the 384kbps (Kilo Bytes per second) service

### **COPYRIGHT INFRINGEMENT**

iBurst is committed to complying with South Africa's copyright and related laws, and requires all customers and users of the Service to comply with these laws. Accordingly, you may not store any material or content on, or disseminate any material or content over, the Service (or any part of the Service) in any manner that constitutes an infringement of third party intellectual property rights, including rights granted in terms of South African copyright law.

Copyright owners may report alleged infringements of their works that are stored on the Service by sending iBurst' authorised agent a notification of claimed infringement. Upon iBurst' receipt of a satisfactory notice of claimed infringement for these works, iBurst will respond expeditiously to either directly or indirectly (i) remove the allegedly infringing work(s) stored on the Service or the Personal Web Features or (ii) disable access to the work(s). iBurst will also notify the affected customer or user of the Service of the removal or disabling of access to the work(s). If the affected customer or user believes in good faith that the allegedly infringing works have been removed or blocked by mistake or misidentification, then that person may send a counter notification to iBurst. Upon iBurst' receipt of a counter notification, iBurst will provide a copy of the counter notification to the person who sent the original notification of claimed infringement. In all events, you expressly agree that iBurst will not be a party to any disputes or lawsuits regarding alleged copyright infringement.

### **PROTECTION OF MINORS**

You must ensure that when children access the internet services are monitored and that they do not access website that have illegal content, including but not limited to pornographic content and gambling. You also guarantee that you will lock the internet Services with a password to prevent unmonitored access.

### **VIOLATION OF ACCEPTABLE AND FAIR USAGE POLICY**

iBurst does not routinely monitor the activity of Service accounts for violation of this AFUP. However, in our efforts to promote good citizenship within the Internet community, we will respond appropriately if we become aware of inappropriate use of our Service. Although iBurst has no obligation to monitor the Service and/or the network, iBurst and its suppliers reserve the right at any time to monitor bandwidth, usage, transmissions, and content from time to time to operate the Service; to identify violations of this AFUP; and/or to protect the network, the Service and iBurst users. iBurst prefers to advise customers of inappropriate behaviour and any necessary corrective action. However, if the Service is used in a way that iBurst or its suppliers, in their sole discretion, believe violate this AFUP, iBurst or its suppliers may take any responsive actions they deem appropriate. These actions include, but are not limited to, temporary or permanent removal of content, cancellation of newsgroup posts, filtering of Internet transmissions, recouping the user terminal device and the immediate suspension or termination of all or any portion of the Service. Neither iBurst nor its affiliates, suppliers, or agents will have any liability for any of the responsive actions. These actions are not iBurst' exclusive remedies and iBurst may take any other legal, technical or financial action it deems appropriate. iBurst reserves the right to investigate suspected violations of this AFUP, including the gathering of information from the user or users involved and the complaining party, if any, and examination of material on iBurst' servers and network. During an investigation, if iBurst decides to investigate, it may suspend the account or accounts involved and/or remove or block material that potentially violates this AFUP. You expressly authorise iBurst and its suppliers to cooperate with law enforcement authorities in the investigation of any suspected legal violations in order to enforce this AFUP. This cooperation may include iBurst providing available personally identifiable information about you to law enforcement or system administrators, including, but not limited to, username, subscriber name, physical address and other account information. Upon termination of your account, iBurst is authorised to delete any files, programs, data and e-mail messages associated with your account. The failure of iBurst or its suppliers to enforce this AFUP, for whatever reason, shall not be construed as a waiver of any right to do so at any time. You agree that if any portion of this AFUP is held invalid or unenforceable, that portion will be construed consistent with applicable law as nearly as possible, and the remaining portions will remain in full force and effect. You agree to indemnify, defend and hold iBurst and its affiliates, suppliers, and agents harmless against all claims and expenses (including legal costs) resulting from you engaging in any of the prohibited activities listed in this AFUP or resulting from your violation of the AFUP or of any other posted iBurst policy related to the Service. Your indemnification will survive any termination of the Subscriber Agreement.

### **ABUSE**

If you suspect that you have been the victim of activities which are in violation of the iBurst AFUP or the Subscriber Agreement, the iBurst Network Abuse Department will take appropriate action to investigate and attempt to resolve

the alleged violation. If you feel that you have been a victim of Internet abuse which took place in part or completely on the iBurst Network, please report the incident to [abuse@iburstgroup.co.za](mailto:abuse@iburstgroup.co.za). If available, please provide the following information:

- the date and time of the alleged violation, including the time zone or offset from GMT
- any evidence of the alleged violation

Emails with full header information provide all of the above, as do syslog files. Other situations will require different methods of providing the above information.

## **MANAGING ABUSE**

When/upon receipt of a complaint, or having become/made aware of an incident, iBurst reserves the right to: Inform the user's network administrator of the incident and require the network administrator or network owner to deal with the incident according to this AFUP.

In the case of individual users iBurst can/will suspend the user's account and withdraw all the user's network access privileges completely.

Institute legal charges against the offending parties for administrative costs as well as for machine and human time lost due to the incident.

Where it is deemed that the cases are severe iBurst will suspend the access of the user's entire network until abuse can be prevented by appropriate means.

Take the appropriate deemed action that may be necessary to protect the integrity of the system, including, but not being limited to, system monitoring, as well as protocol management and shutting down of ports affected by viruses, worms or other malicious code.

Implement appropriate technical mechanisms and other processes in order to prevent usage patterns that may violate this AFUP.

Share information concerning the incident with other Internet access providers, or publish the information, and/or make available the users' details to law enforcement agencies.

Any one or more of the steps listed above, in so far as they are deemed necessary by iBurst in its absolute and sole discretion, may be taken by iBurst against the offending party.