



ACCEPTABLE USAGE TERMS

DATE OF LAST REVIEW: 25 SEPTEMBER 2018

IMPORTANT PLEASE NOTE: This Acceptable Usage Terms document will be updated intermittently. Please ensure that this document is reviewed from time to time to remain abreast of content and legalities.

TABLE OF CONTENTS

General	3
Ispa Membership And Code Of Conduct	4
Acceptable Use	4
Unlawful/Unacceptable Use	4
Fair Usage Policy	5
Prohibited Activities	5
Threats To Network Security	5
Spam And Bulk Mail	6
Spam/Virus Filtering	7
Public Space And Third-Party Content And Sites.....	7
User Responsibilities.....	8
Users Outside Of South Africa	8
Protection Of Minors	8
Privacy And Confidentiality	9
Notice And Take Down Procedures	9
Complaints Procedure	9
Action Following Breach Of The Aup	9

GENERAL

The Kibo Connect (otherwise referred to as “Kibo”) Acceptable Usage Policy (“AUP”) is a legal document which stipulates the constraints and practices that a user must agree to for access to a corporate network or the Internet as governed by local regulation e.g. ICASA, ECA etc.

Thank you for taking the time to read the Kibo AUP. By accessing this website, or by contracting with us for service, you agree, without limitation or qualification, to be bound by this policy and the terms and conditions it contains, as well as any other additional terms, conditions, rules or policies which are displayed to you in connection with this service/website. This document sets out in detail to define acceptable behaviour and the general conduct which is regarded as unacceptable by Kibo and the repercussions of said actions regarding the unacceptable use of the services. This is important to:

- Specify to Customers and users of our service/website what activities and online behaviour are considered an unacceptable use of the service/website
- Protect our Customers and infrastructure from abuse;
- Adhere to the current laws and regulations governing organisations and service providers in the countries that we operate in;
- Protect and maintain the integrity of our network and to specify the consequences that may flow from undertaking such prohibited activities;
- Co-exist within the global Internet community as a responsible service provider.

The Customer is expected to use the Internet and other networks/services with respect, courtesy, and responsibility, giving due regard to the rights of other Internet users. Common sense is the best guide as to what is considered acceptable use.

Kibo Connect reserves the right to amend the AUP as required. Updated versions will be posted on the Kibo site and can be located at www.kiboconnect.co.za/legal. The Customer usage of the Kibo Connect services will constitute acceptance of amended terms once posted on the official Kibo website.

This document contains several legal obligations which the Customer will be presumed to be familiar with. As such, Kibo Connect encourages the Customer to read this document thoroughly and direct any queries to info@kiboconnect.co.za.

Kibo Connect respects the rights of our Customers and users of our services to freedom of speech and expression; access to information; privacy; human dignity; religion, belief and opinion in accordance with the South African constitution. We undertake not to interfere with any of those rights unless required to do so by law; unless those rights are exercised for unlawful purposes; or unless the exercise of those rights threatens to cause harm to another person or affect the integrity of our network.

ISPA MEMBERSHIP AND CODE OF CONDUCT

Kibo Connect confirms that in compliance with section 72 of the Electronic Communications and Transactions Act 25 of 2002, Kibo Connect is a member of the Internet Service Providers' Association (ISPA) and has adopted and implemented the association's official Code of Conduct, which can be viewed at www.ispa.org.za/code-of-conduct.

ACCEPTABLE USE

Acceptable use starts at the first second on the first day of a month and ends at midnight on the last day of the same month.

All Customers who use Kibo's infrastructure agree not to use it in any way that goes against appropriate laws or regulations. If Kibo is given a legally binding court order for a user, their personally-identifiable information will be given to law-enforcement agencies.

UNLAWFUL/UNACCEPTABLE USE

Kibo Connect's services/website may only be used for lawful purposes and activities. We prohibit any use of our website/network including the transmission, storage and distribution of any material or content using our network that violates any law or regulation of the Republic.

The following sections outline activities that are considered an unacceptable use of Kibo Connect's services/network/website and also detail the guidelines for acceptable use of certain facilities/services, as the case may be. This includes:

- Any violation of local and international laws prohibiting child pornography; obscenity; discrimination (including racial, gender or religious slurs) and hate speech; or speech designed to incite violence or hatred, or threats to cause bodily harm;
- Kibo Connect's IP Services shall not be used in connection with any criminal, civil or administrative violation of any applicable local, provincial, national or international law, treaty, court orders, ordinance, regulation or administrative rules;
- Any activity designed to defame, abuse, stalk, harass or physically threaten any individual in the Republic of South Africa or beyond its borders; including any attempt to link to, post, transmit or otherwise distribute any inappropriate or defamatory material;
- Kibo Connect's IP Services shall not be used to host, post, transmit, or re-transmit any content or material (or to create a domain name or operate from a domain name), that harasses, or threatens the health or safety of others. In addition, for those IP Services that utilize Kibo Connect provided web or content hosting, Kibo reserves the right to decline to provide such services if the content is determined by Kibo to be obscene, indecent, hateful, malicious, racist, defamatory, fraudulent, libellous, treasonous, excessively violent or promoting the use of violence or otherwise harmful to others;
- Any violation of Intellectual Property laws including materials protected by local and international copyright, trademarks and trade secrets. Moreover, Kibo Connect cannot be held liable if you make any unlawful use of any multimedia content accessed through the search facility provided by Kibo Connect's network, or otherwise available through access to our network, whether for commercial or non-commercial purposes. **Specifically**, Kibo Connect's IP Service(s) shall not be used to publish, submit/receive upload/download, post, use, copy or otherwise reproduce, transmit, re-transmit, distribute or store any content/material or to engage in any activity that infringes, misappropriates or otherwise violates the intellectual property rights or privacy or publicity rights of Kibo or any individual, group or entity, including but not limited to any rights protected by any copyright, patent, trademark laws, trade secret, trade dress, right of privacy, right of publicity, moral rights or other intellectual property right now known or later recognized by statute, judicial decision or regulation;
- Any violation of the individual's right to privacy, including any effort to collect personal data of third parties without their consent;

KIBO CONNECT ACCEPTABLE USAGE TERMS

- Any fraudulent activity whatsoever, including dubious financial practices, such as pyramid schemes; the impersonation of another subscriber without their consent; or any attempt to enter into a transaction with Kibo Connect on behalf of another subscriber without their consent;
- Any violation of the exchange control laws of the Republic;
- Any activity that results in the sale, transmission or distribution of pirated or illegal software;
- Failing to respond to a request by a recipient of unsolicited mail to be removed from any mailing or direct marketing list and continuing to send unsolicited mail following such a request for removal;
- Where any user resides outside of the Republic, permanently or temporarily, such user will be subject to the laws of the country in which s/he is currently resident, and which apply. On presentation of a legal order to do so, or under obligation through an order for mutual foreign legal assistance, Kibo Connect will assist foreign law enforcement agencies (LEA) in the investigation and prosecution of a crime committed using, Kibo Connect's resources, including the provisioning of all personal identifiable data.

FAIR USAGE POLICY

This Fair Usage Policy (FUP) applies only to Kibo Connect uncapped consumer Internet services. These services include ADSL, VDSL and FTTH. Customers need to select the appropriate solution for their access port speed and type of usage application.

Kibo Connect reserves the right to apply restrictions on an uncapped Internet account if a customer's behaviour is determined to be affecting the user experience of other customers on Kibo Connect's network. Such restrictions may include but are not limited to throttling a customer's throughput speeds to an appropriate proportion of the actual port speed and / or shaping a customer's bandwidth to limit the use of bandwidth intensive protocols and applications.

Examples of customer behaviour which may compromise Kibo Connect's network performance include, for example, causing network congestion, running excessive concurrent internet sessions or accessing excessive bandwidth intensive protocols such as peer-to-peer.

In the event of such behaviours, Kibo Connect reserves the right to ultimately terminate the account of a customer whose usage is continuously affecting Kibo Connect's network performance.

The provisions of this AUP are intended as guidelines and are not meant to be exhaustive. Generally, conduct that violates law, regulation, or the accepted norms of the Internet community, whether expressly mentioned in this AUP, is prohibited. Kibo Connect reserves the right always to prohibit activities that damage its commercial reputation and goodwill.

PROHIBITED ACTIVITIES

The following sections outline activities that are considered an unacceptable use of Kibo Connect's services/network/website and detail the guidelines for acceptable use of certain facilities/services, as the case may be.

THREATS TO NETWORK SECURITY

Any activity which threatens the functioning, security and/or integrity of Kibo Connect's network is unacceptable. This includes:

- Any efforts to attempt to gain unlawful and unauthorised access to the network or circumvent any of the security measures established by Kibo Connect for this goal;
- Impersonating others or secretly or deceptively obtaining personal information of third parties (phishing, etc.);
- Interference with service to any user, host or network including, without limitation, mail bombing, flooding, deliberate attempts to overload a system and broadcast attacks;

KIBO CONNECT ACCEPTABLE USAGE TERMS

- Utilising any program, file, script, command or transmission of any message or content of any kind, designed to interfere with a terminal session, the access to or use of the Internet or any other means of communication;
- Any effort to use Kibo Connect's equipment to circumvent the user authentication or security of any host, network or account ("cracking" or "hacking"), attacking, gaining access to, breaching, circumventing or testing the vulnerability of the user authentication or security of any host, network, server, personal computer, network access and control devices, software or data without express authorization of the owner of the system or network;
- Forging of any TCP/IP packet headers (spoofing) or any part of the headers of an email or a newsgroup posting;
- Any effort to breach or attempt to breach the security of another user or attempt to gain access to any other person's computer, software, or data without the knowledge and consent of such person;
- Distributing or using tools designed to compromise security (including but not limited to SNMP tools), including cracking tools, password guessing programs, packet sniffers or network probing tools (except in the case of authorized legitimate network security operations);
- Any activity which threatens to disrupt the service offered by Kibo Connect through "denial of service attacks"; flooding of a network, or overloading a service or any unauthorised probes ("scanning" or "nuking") of others' networks;
- Any activity which in any way threatens the security of the network by knowingly posting, uploading, transmitting, linking to or otherwise distributing any information or software which contains a virus, trojan horse, time bombs, cancel bots, corrupted files, root kits, worm, malware, botnet or other harmful, destructive or disruptive component which may damage the operation of another's computer, network system or other property, or be used to engage in modem or system hi-jacking;
- Any unauthorised monitoring of data or traffic on the network without Kibo Connect's explicit, written consent;
- Running services and applications with known vulnerabilities and weaknesses, e.g. insufficient anti-automation attacks, any traffic amplification attacks, including recursive DNS attacks, SMTP relay attacks;
- Failing to respond adequately to a denial of service attack (DOS / DDOS).
- Any unsolicited mass mailing activity including direct marketing; SPAM and chain letters for commercial or other purposes, without the consent of the recipients of those mails;
- Employing posts or programs which consume excessive CPU time or storage space, permits the use of mail services, mail forwarding capabilities, POP accounts, or auto responders other than for their own account; or resale of access to CGI scripts installed on our servers.

SPAM AND BULK MAIL

SPAM and unsolicited bulk mail are highly problematic practices. They affect the use and enjoyment of services by others and often compromise network security. Kibo Connect will take swift and firm action against any user engaging in any of the following unacceptable practices:

- Sending unsolicited bulk mail for marketing or any other purposes (political, religious or commercial) to people who have not consented to receiving such mail;
- A user shall not use another site's mail server to relay mail without the express permission of the site or distributing, advertising or promoting software or services that have the primary purpose of encouraging or facilitating unsolicited commercial email or SPAM;
- Operating or maintaining mailing lists without the express permission of all recipients listed;
- Failing to promptly remove from lists invalid or undeliverable addresses or addresses of unwilling recipients;
- To engage in any of the foregoing activities using the service of another provider, but channelling such activities through a Kibo-provided server, or using a Kibo-provided server as a maildrop for responses;

KIBO CONNECT ACCEPTABLE USAGE TERMS

- To falsify user information provided to Kibo Connect or to other users of the service in connection with use of a Kibo service;
- Using Kibo Connect's service to collect responses from unsolicited e-mail sent from accounts on other Internet hosts or e-mail services, that violate this AUP or the AUP of any other Internet service provider;
- Including Kibo Connect's name in the header or by listing an IP address that belongs to Kibo Connect in any unsolicited email sent through Kibo Connect's network or not;
- Failure to secure a Customer's mail server against public relay as a protection to themselves and the broader Internet community. Public relay occurs when a mail server is accessed by a third party from another domain and is utilised to deliver mails, without the authority or consent of the owner of the mail-server. 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. Kibo Connect reserves the right to examine users' mail servers to confirm that no mails are being sent from the mail server through public relay and the results of such checks can be made available to the user. Kibo Connect also reserves the right to examine the mail servers of any users using Kibo Connect's mail servers for "smart hosting" (when the user relays its mail via a Kibo Connect mail server to a mail server of its own) 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 Kibo Connect's privacy policy.

Kibo Connect's Customers should never reply to SPAM, because this usually only confirms that your address is working and will lead to more SPAM being sent. We also strongly discourage users from buying lists of e-mail addresses for marketing or advertising because these lists are usually fraudulent and are made up of addresses that were gained by dishonest, untrustworthy or unethical means.

SPAM/VIRUS FILTERING

Kibo Connect provides a SPAM and virus filtering system to protect Customers from unsolicited mail and viruses. The Customer acknowledges that this system might incorrectly identify a valid message as SPAM or as a virus and consequently this message might not be delivered to the Customer. The Customer acknowledges and agrees that Kibo Connect shall without limitation have no responsibility for, or liability in respect of any data lost as a result of this system. Kibo Connect reserves the right to examine incoming or outgoing mail to the extent necessary to determine if it is classified as SPAM.

Kibo Connect regards all unsolicited bulk email (whether commercial in nature or not) as SPAM, with the following exceptions:

- Mail sent by one party to another where there is already a prior relationship between the two parties and the subject matter of the message(s) concerns that relationship;
- Mail sent by one party to another with the explicit consent of the receiving party;
- Customers should only receive bulk mail that they have requested and/or consented to receive and/or which they would expect to receive as a result of an existing relationship.

Kibo Connect will take swift and firm action against any user engaging in any of the following unacceptable practices relating to SPAM as per the above unlawful/unacceptable policies.

PUBLIC SPACE AND THIRD-PARTY CONTENT AND SITES

In reading this AUP or in signing a service contract with Kibo Connect, you acknowledge that Kibo Connect has no power to control the content of the information passing over the Internet and its applications, including e-mail; chatrooms; news groups; or other similar fora, and that Kibo Connect cannot be held responsible or liable, directly or indirectly, for any of the abovementioned content, in any way for any loss or damage of any kind incurred as a result of, or in connection with your use of, or reliance on, any such content.

Our services also offer access to numerous third-party webpages. You acknowledge that we exercise absolutely no control over such third-party content, or sites and in such cases, our network is merely a conduit or means of access and transmission. This includes, but is not limited to, third party content contained on or accessible through

the Kibo Connect network websites and web pages or sites displayed as search results or contained within a directory of links on the Kibo Connect network. It remains your responsibility to review and evaluate any such content, and that all risk associated with the use of, or reliance on, such content rests with you.

Access to public Internet spaces, such as bulletin boards, Usenet groups, chat rooms and moderated forums is entirely voluntary and at your own risk.

Kibo Connect employees do not moderate any of these services, or your communications, transmissions or use of these services. We do not undertake any responsibility for any content contained therein, or for any breaches of your right to privacy that you may experience because of accessing such spaces.

USER RESPONSIBILITIES

Customers are responsible for any misuse of Kibo Connect's services that occurs through the Customer's account. It is the Customer's responsibility to ensure that unauthorised persons do not gain access to or misuse any Kibo Connect services.

Kibo Connect urges Customers not to reply to unsolicited mail or "SPAM", not to click on any suggested links provided in the unsolicited mail. Doing so remains the sole responsibility of the Customer and Kibo Connect cannot be held liable for the Customer being placed on any bulk mailing lists as a result.

Where the Customer has authorised a minor to use any of the Kibo Connect's services or access its websites, you accept that as the parent/legal guardian of that minor, you are fully responsible for: the online conduct of such minor; controlling the minor's access to and use of any services or websites; and the consequences of any misuse by the minor, including but not limited to transactions entered into by the minor using such access.

Kibo Connect cannot be held liable for any business dealings you have with any third parties on the Internet, including any vendors, or advertisers found on, or through, the Kibo Connect network. Further, Kibo Connect assumes no responsibility whatsoever for any charges you or any user of your account incurs when making purchases or other transactions in this manner. Further, the responsibility for ensuring compliance with all applicable customs and exchange control laws in connection with any such transactions shall be the Customer's.

Customers remain solely and fully responsible for the content of any material posted, hosted, downloaded/uploaded, created, accessed or transmitted using Kibo Connect services.

Customers are responsible for taking prompt corrective action(s) to remedy a violation of AUP and to help prevent similar future violations.

USERS OUTSIDE OF SOUTH AFRICA

Where any user resides outside of the Republic, permanently or temporarily, such user will be subject to the laws of the country in which s/he is currently resident, and which apply to the user. On presentation of a legal order to do so, or under obligation through an order for mutual foreign legal assistance, Kibo Connect will assist foreign law enforcement agencies (LEAs) in the investigation and prosecution of a crime committed using Kibo Connect's resources, including the provisioning of all personal identifiable data.

PROTECTION OF MINORS

Kibo Connect prohibits Customers from using Kibo Connect's service to harm or attempt to harm a minor, including, but not limited to, by hosting, possessing, disseminating, distributing or transmitting material that is unlawful, including child pornography and cyber bullying.

Kibo Connect prohibits Customers from using Kibo Connect's service to host sexually explicit or pornographic material of any nature.

Kibo Connect services should not be used for the commission an offence against a child or in way that would constitute or promote unlawful interaction with children.

Kibo Connect services shall not be used to publish, submit/receive, upload/download, post, use, copy or otherwise produce, transmit, distribute or store child pornography. Suspected violations of this prohibition may be reported to Kibo Connect at the following e-mail address: abuse@kiboconnect.com. Kibo Connect will report any discovered

violation of this prohibition to the South African Police services and take steps to remove child pornography (or otherwise block access to the content determined to contain child pornography) from its servers.

PRIVACY AND CONFIDENTIALITY

Kibo Connect respects the privacy and confidentiality of our Customers and users of our service. Please review our privacy policy which details how we collect and use personal information gathered in the course of operating this service.

NOTICE AND TAKE DOWN PROCEDURES

Kibo Connect confirms that it has a procedure in place for the notice and take-down of illegal material. In compliance with section 77 of the *Electronic Communications and Transactions Act (No. 25 of 2002)* Kibo Connect's designated agent for this process can be reached at (010) 500 1200 or at takedown@ispa.org.za. The notice and take-down procedure can be viewed at www.ispa.org.za/code-of-conduct.

Customers are also notified of the content and procedures of the ISPA Code of Conduct (<http://ispa.org.za/code-of-conduct/request-a-take-down/>) which may be used against any Internet service provider who fails to comply with the code of conduct. We urge you to familiarise yourselves with this code.

COMPLAINTS PROCEDURE

Complaints relating to the violation of this AUP should be submitted in writing to abuse@kiboconnect.co.za. Complaints must be substantiated, and unambiguously state the nature of the problem, and its connection to Kibo Connect's network and services.

It is the Customer's responsibility to familiarise himself or herself with the procedure set out below and report any cases of violation of this AUP to Kibo Connect's designated complaints handling agent.

Please note that Kibo Connect cannot handle complaints concerning networks or users that do not have service contracts with us or our affiliates or are outside of our control.

For Kibo Connect to thoroughly investigate the complaint and take appropriate action, all complaints must be in writing, via fax or e-mail and contain as much information as possible, including, but not limited to:

- The origin of abuse or offence, including the website, full mail headers, relevant logfile extracts etc.;
- Any contact details for the source of the complaint;
- A brief explanation why the incident is an offence.

Kibo Connect discourages anonymous complaints being made via this service and urges complainants to supply their name and contact details to us. Such information will not be released, except where required by law enforcement. Anonymous complaints will however be acted upon as long as sufficient detail as outlined above is supplied.

ACTION FOLLOWING BREACH OF THE AUP

Upon receipt of a complaint, or having become aware of an incident, Kibo Connect may, in its sole and reasonably-exercised discretion take any of the following steps:

- In the case of Customers, warn the Customer, suspend the Customer account and/or revoke or cancel the Customer's Service access privileges completely;
- In the case of abuse emanating from a third party, inform the third party's network administrator of the incident and request the network administrator or network owner to address the incident in terms of this AUP and/or the ISPA Code of Conduct (if applicable);
- In severe cases suspend access of the third party's entire network until abuse can be prevented by appropriate means;
- In all cases, charge the offending parties for administrative costs as well as for machine and human time lost due to the incident;

KIBO CONNECT ACCEPTABLE USAGE TERMS

- Assist other networks or website administrators in investigating credible suspicions of any activity listed in this AUP;
- Institute civil or criminal proceedings;
- 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; and/or suspend or terminate the Service as provided for in the Agreement;
- This policy applies to and will be enforced for intended and unintended (e.g., viruses, worms, malicious code, or otherwise unknown causes) prohibited usage.

Kibo Connect will be the sole arbiters and have a sole and unfettered discretion in determining what constitutes a violation of this AUP.

Once Kibo Connect becomes aware of an alleged violation of its AUP, Kibo will initiate an investigation. During the investigation, Kibo may restrict the user's access to prevent further possible unauthorised activity.