

General Notice

Thank you for reading Iclix's Acceptable Use Policy (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.

The purpose of this AUP is to comply with the relevant laws of the Republic; to specify to clients and users of our service/website what activities and online behavior are considered an unacceptable use of the service/website; to protect the integrity of our network and to specify the consequences that may flow from undertaking such prohibited activities. This document contains a number of legal obligations which you are presumed to be familiar with. As such, we encourage you to read this document thoroughly and direct any queries to our client services/legal department at 0514006900

Iclix respects the rights of our clients and users of our services to freedom of speech and expression; access to information; privacy; human dignity; religion, belief and opinion in accordance with our 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 Iclix confirms that in compliance with section 72 of the Electronic Communications and Transactions Act 25 of 2002, Iclix 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

Unlawful Use

Iclix'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.

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.

Any activity designed to defame, abuse, stalk, harass or physically threaten any individual in the Republic or beyond its borders; including any attempt to link to, post, transmit or otherwise distribute any inappropriate or defamatory material.

Any violation of Intellectual Property laws including materials protected by local and international copyright, trademarks and trade secrets. Moreover Iclix cannot be held liable if you make any unlawful use of any multimedia content accessed through the search facility provided by Iclix's network, or otherwise available through access to our network, whether for commercial or noncommercial purposes.

Any violation of the individual's right to privacy, including any effort to collect personal data of third parties without their consent. 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 Iclix 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, Iclix will assist foreign law enforcement agencies (LEA) in the investigation and prosecution of a crime committed using Iclix's resources, including the provisioning of all personal identifiable data.

Prohibited Activities

The following sections outline activities that are considered an unacceptable use of Company's services/network/website and also 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 Iclix's network is unacceptable.

This includes:

Any efforts to attempt to gain unlawful and unauthorized access to the network or circumvent any of the security measures established by Iclix for this goal; Any effort to use Iclix's equipment to circumvent the user authentication or security of any host, network or account ("cracking" or "hacking"); Forging of any TCP-IP packet header (spoofing) or any part of the header information in 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; Any activity which threatens to disrupt the service offered by Iclix through "denial of service attacks", flooding of a network, or overloading a service or any unauthorized probes ("scanning" or "nuking") of others' networks; Any activity which in any way threatens the security of the network by knowingly posting, transmitting, linking to or otherwise distributing any information or software which contains a virus; Trojan horse; worm, lock, mail bomb, cancel bot or other harmful, destructive or disruptive component.

Any unauthorised monitoring of data or traffic on the network without Iclix's explicit, written consent. 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.

Public Space & Third Party Content & sites

In reading this AUP or in signing a service contract with Iclix, you acknowledge that Iclix has no power to control the content of the information passing over the Internet and its applications, including e-mail; chat rooms; news groups; or other similar fora, and that Iclix 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 Iclix network websites and web pages or sites displayed as search results or contained within a directory of links on the Iclix network. It remains your responsibility to review and evaluate any such content, and that any and 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.

Iclix 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 as a result of accessing such spaces.

Newsgroups

The client is responsible for determining and familiarizing himself or herself with the written policies of a given newsgroup before posting to it. The client must comply with these guidelines at all times which can be obtained from other users of the newsgroup upon request, or from the group's administrators/moderators. The following are prohibited practices with regard to Usenet newsgroups and Iclix reserves the right to delete and/or cancel posts which violate the following conditions:

Excessive cross-posting of the same article to multiple newsgroups. Posting of irrelevant or off-topic material to newsgroups (also known as USENET spam).

Posting binaries to a non-binary newsgroup. Posting adverts, solicitations, or any other commercial messages unless the guidelines of the newsgroup in question explicitly permit them. Iclix does not monitor nor control the content that is available or unavailable via newsgroup and/or usenet services. The services offered by Iclix in respect to usenet services is merely a convenience to Iclix clients to make the use of the service more convenient. Iclix accepts no liability and has no control over the content that may or may not be available, including, but not limited to, pornography, illegally obtained movies, applications and music. Unsolicited, Spam and Junk 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. Iclix 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; 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; Using Iclix'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 Iclix's name in the header or by listing an IP address that belongs to Iclix in any unsolicited email sent through Iclix's network or not; Failure to secure a client'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 utilized 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. Iclix 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. Iclix also reserves the right to examine the mail servers of any users using Iclix's mail servers for "smart hosting" (when the user relays its mail via a Iclix 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 Iclix's privacy policy.

Free Email Account

Iclix provides up to 5 free email addresses per profile/client. The email address is provided free of charge and will remain active even in the event of the client cancelling their services. The email account must send or download an email at least once within a 6 month period; failing this the email address will be deleted and become available to other users. This service is strictly available for individual's personal use and must in no way be used for business purposes. Should you require an email address for business purposes please have a look at our Hosting Services. Please ensure that you familiarize yourself with the Spam/Virus Filtering and Webmail sections here-under should you choose to make use of this service.

Spam/Virus Filtering

Iclix provides a spam and virus filtering system to protect clients from unsolicited mail and viruses. The client 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 client. The client acknowledges and agrees that Iclix shall without limitation have no responsibility for, or liability in respect of any data lost as a result of this system.

Webmail

Webmail and other web based email services made available by Iclix are provided on an "as is" basis without representations, warranties or conditions of any kind, and the client acknowledges and agrees that Iclix shall have no responsibility for, or liability in respect of, any aspect of the Webmail services, including without limitation for any lost or damaged data or any acts or omissions of Iclix. As webmail storage space is limited, some Webmail messages may not be processed due to space constraints or message limitations.

Webmail is provided to individuals and for personal use only. Any unauthorised commercial use of the Webmail service, or resale of the Webmail service is expressly prohibited.

Uncapped Services

It is our goal to protect the integrity of our network, in order to provide the best possible internet experience for all of our clients using all Uncapped services and as such we reserve the right to manage uncapped users who are deemed to be causing an unusually large burden on the network. We are committed to managing our network in a way that allows us to provide all users with the best experience possible, however we cannot guarantee that the allocated capacity will always be available.

Home Uncapped / Premium Uncapped

Home Uncapped services are best suited for average home users who make little to no use of high bandwidth services such as NNTP, Peer-to-Peer and Torrents (and similar but not limited to). Home Uncapped services are proactively managed by the Iclix Protocol Manager. Premium Uncapped services are better suited to more advanced users, and are managed proactively by the Iclix Protocol Manager. Premium Uncapped (DSL and Fibre) - Iclix Protocol Manager The Iclix Protocol Manager is used to provide all uncapped users on our network with the best possible internet experience. During peak network times, we give priority to real time services (such as browsing, email, streaming etc), high bandwidth services such as NNTP, Peer-to-Peer and Torrents (and similar but not limited to) will receive less priority. Clients deemed to be continuously uploading/downloading or using the service for unattended automated processes will be managed by the Iclix Protocol Manager. The Iclix Protocol Manager may be used to manage clients by rate limiting (slowing down speed) and limiting or preventing service using specific protocols or ports. We reserve the right to use the Iclix Protocol Manager to manage the integrity of our network should network capacity not be available at any time, we assure our clients that we will do this in a responsible manner should the need arise. Any user that is found attempting to bypass or circumvent the Iclix Protocol Manager will be suspended and could have their service cancelled.

Home Uncapped (DSL and Fibre) – Iclix Protocol Manager

Home Uncapped services are managed according to the last 7 days usage projected to 30 days as well as the available capacity on the network at all times. There are predefined thresholds set and when exceeded the account speed will be managed down to a maximum of 50% of the account speed. Should the demand on the network exceed available capacity these thresholds may be managed more aggressively by the Iclix Protocol Manager and differ to the table below.

The thresholds per account speed are:

Speed	Threshold
1Mbps	20GB
2Mbps	40GB
4Mbps	80GB
8Mbps	100GB
10Mbps	120GB
20Mbps	200GB
40Mbps	400GB
100Mbps	800GB

Any user that is found attempting to bypass or circumvent the Iclix Protocol Manager will be suspended and could have their service cancelled. Business Uncapped (DSL and Fibre) This is an uncapped service that is prioritized for Business Users based on available network capacity where high priority is required for typical business protocols. Clients deemed to be continuously uploading/downloading or using the service for unattended automated processes or non-typical business protocols (such as but not limited to NNTP, Peer-to-Peer, Https Downloading and Torrents) will be managed by the Iclix protocol Manager. The Iclix Protocol Manager may be used to manage clients by rate limiting (slowing down speed) and

limiting or preventing service using specific protocols or ports. Iclix reserves the right, to at its discretion manage non typical business protocols such as but not limited to NNTP, Peer-to-Peer, Https Downloading and Torrents and/or rate limit service speed. We reserve the right to use the Iclix Protocol Manager to manage services in order to protect the integrity of our network according to the available network capacity, we assure our clients that we will do this in a responsible manner should the need arise. Any user that is found attempting to bypass or circumvent the Iclix Protocol Manager will be suspended and could have their service cancelled.

Hosting

Iclix offers unlimited bandwidth (web traffic) usage on Shared Hosting platforms. However, this is subject to reasonable and responsible usage, as determined at Iclix' discretion. Shared Hosting is designed for serving personal hosting requirements or that of small enterprises, and not medium to large enterprises. Iclix reserves the right to move Clients deemed to have excessive bandwidth usage to a Cloud product, which will better suit their requirements. Clients will be given notice as such, and will be informed of any cost implications. Disk Space on Shared Hosting may only be used for Website Content, Emails and related System Files. General data storage, archiving or file sharing of documents, files or media not directly related to the website content is strictly prohibited. Unauthorised storage or distribution of copyrighted materials is prohibited, via FTP hosts or any other means. For Shared Hosting, Iclix will implement security updates, software patches and other updates or upgrades from time to time, to maintain the best performance, at their sole discretion. Iclix is under no obligation to effect such upgrades, or to rectify any impact such changes could potentially have to Shared Hosting Clients. Iclix will not be liable responsible for the backing up, restoration or loss of data under any circumstances. Clients are solely responsible for ensuring their data is regularly backed up and for restoring such backups in the event of data loss or corruption. Iclix prohibits Clients from doing the following on hosting platforms administered by Iclix:

Running applications that are not production-ready. Any applications on the hosting platform must be optimized with respect to memory usage and must have appropriate data indexing. Running applications with inadequate security controls.

Generating significant side-channel traffic from an application, whether by design or otherwise. Databases should be stored locally, and remote content should be cached. Failure to maintain proper "housekeeping" on a shared server including storing or generating useless content, including comment spam, unused cache files, log file and database entries.

Storing malicious content, such as malware or links to malware. Monopolizing server resources, including CPU time, memory, network and disk bandwidth. Maintaining long-running processes and long-running database queries. Storing or running back-door shells, mass mailing scripts, proxy servers, web spiders, phishing content, or peer-to-peer software.

Sending bulk mail of any form, particularly mail that cannot be efficiently delivered due to volume or incorrect addresses.

Using poor passwords. Sharing security credentials with untrusted parties. Running Torrents for download or Seed Servers.

Running TOR (or other Online Anonymity Services). Otherwise circumventing the Acceptable Use Policy or intended use of the product.

Protection of Minors

Iclix prohibits clients from using Iclix'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.

Privacy and Confidentiality

Iclix respects the privacy and confidentiality of our clients 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.

User Responsibilities

Clients are responsible for any misuse of Company's services that occurs through the client's account. It is the client's responsibility to ensure that unauthorised persons do not gain access to or misuse Iclix's service. Iclix urges clients 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 client and Iclix cannot be held liable for the client being placed on any bulk mailing lists as a result.

Where the client has authorised a minor to use any of the Iclix'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. Iclix 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 Iclix network. Further, Iclix 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 client's.

Notice and Take-down Procedures

Iclix 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) Iclix's designated agent for this process can be reached at (051) 400 6900 or at: complaints@iclix.co.za, The notice and take-down procedure can be viewed at www.ispa.org.za/code. Clients are also notified of the content and procedures of the ISPA Code of Conduct (www.ispa.org.za/code) 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 and procedures

It is the client's responsibility to familiarise himself or herself with the procedure set out below and report any cases of violation of this AUP to Iclix's designated complaints handling agent. Please note that Iclix cannot handle complaints concerning networks or users that do not have service contracts with us or our affiliates, or are outside of our control.

In order for Iclix 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 considered to be an offence. Iclix 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, Iclix may take any of the following steps:

In the case of a network, inform the user's network administrator of the incident and request the network administrator or network owner to deal address the incident in terms of this AUP and the ISPA Code of Conduct; In severe cases suspend access of the user's entire network until abuse can be prevented by appropriate means; In the case of individual users, warn the user; suspend the user's account and/or revoke or cancel the user's network access privileges completely; In all cases, charge the offending parties for administrative costs as well as for machine and human time lost due to the incident;

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

Reservation and Non Waiver of Rights

Iclix reserves the right to amend or alter this policy at any time, and without notice to you. Iclix reserves the right to take action against any individuals, companies or organizations that violate any of the prohibited activities set out herein, or engage in any illegal or unlawful activity while accessing our services, to the fullest extent of the law. Iclix reserves the right, at its sole discretion, to act against other types of abuse not listed in this document and to investigate or prevent illegal activities being committed over our network. Iclix reserves the right to monitor user and network traffic for site security purposes and prevent any unauthorised attempts to tamper with our site or cause damage to our property. Iclix reserves the right to suspend, revoke or cancel Iclix's services to the client/user if the safety and integrity of Iclix's resources are placed at risk in continuing to provide service to the subscriber/user. Iclix reserves the right to remove any information or materials in whole or in part, that, in Iclix's sole discretion, is deemed to be offensive, indecent, or otherwise objectionable. Iclix does not undertake to guarantee the security of any data passing through its networks. Although Iclix will provide a "best effort" service, including regular updates on computer viruses and other threats to security of data, it is the responsibility of the communicating parties to safeguard their data, and Iclix cannot be held liable for any loss or damage arising as result of the failure to do so. Iclix does not waive its right to enforcement of this AUP at any time, or prejudice its right to take subsequent action, should Iclix fail, neglect or elect not to enforce a breach of the AUP at any time.

Fibre Services

Fibre Broadband Access is supplied as a best effort service by the supplier. Areas marked as available on the map may not be Fibre ready at your particular address due to a number of factors. Should we not be able to proceed with your application we will advise you thereof. Installations are typically completed within +/- 30 days, this timeframe is however not guaranteed. Fibre installations are subject to an installation and connection fee. Additional fees may apply should trenching be required to complete the installation, Iclix will make any additional charges known to the client and the client will be required to accept or reject these charges before the order is completed. Please note that should the service be ordered and the incorrect address is supplied, the client will be responsible for all charges relating to the order placed at the incorrect address. An additional fee will be charged for re-grading the speed of a fibre line as well as outdoor transfers (new address) and transfers between Service Providers. Cancellations for fibre lines are only submitted at the end of each month, the cancellation request must be submitted via the Client Control Panel at least 30 calendar days before the cancellation date, the earliest available cancellation date will be shown in the Client Control Panel. Transfers between Service Providers are handled in the same manner as a new installation and are typically completed within +/- 30 day, this timeframe is however not guaranteed. An additional fee of up to R2 000.00 may be charged on faults logged which are found to be caused by faulty hardware or user error. This amount will be charged to your account once we are advised of the charges by the Supplier. By completing the order it is deemed that consent has been received from the landlord, owner or body corporate for the installation of the service. The available capacity on the network is shared between all users of Iclix bandwidth. Acceptable Usage Policies are attached to Uncapped Services. Capped services whilst the majority of the time will remain untouched may be shaped or throttled should the demand on the network and available capacity be affected. Capped services will generally receive priority through-put on our network provided there is no rise in demand or extenuating circumstances affecting the performance of the network.

Capped Services

Rollover of Data

Should you not use all of your purchased data within a month (1st to last day of each month); the unused data will carry over to the following month for a period of 3 months. As your data is exhausted the unused data from the oldest months

accumulated data will be added to your service. In order to use your rollover you must first deplete your monthly allocation of data, once the monthly allocation is depleted your rollover data will automatically become available.

EXAMPLE

You have not used up all your data for June, July and August. In September you run out of data, we will automatically allocate the unused data from June to your data service first. If you deplete this data too, we will automatically allocate the unused data from July and if you deplete this, we will automatically allocate the data from August. If you reach the end of September and you only needed to use your rollover data from June and July, the unused data from August will be available to use in October. Rollover of Data is only applicable to services which are paid up to date and are renewed monthly. If your debit order or credit card payment fails for any reason all data that has accumulated will fall away and will not be re-allocated on payment for the service. Should you cancel your service any accumulated data will fall away.

Uncapped Services

Uncapped services are designed and intended for personal use only. The Uncapped Services may not be repackaged/broken down and sold to 3rd parties, may not be used to provide network services like hosting/mail/ftp/backhaul for Wifi/internet cafes and other networks. The use and/or exploitation of our uncapped services for commercial use is strictly prohibited. (We have very competitive Per Gb pricing for commercials). The Acceptable Use Policy for the Home Uncapped, Premium Uncapped and Business Uncapped can be found here. By accepting the Terms and Conditions, you also agree to the aforementioned AUP. All uncapped services are billed within a calendar month (1st to last day of every month). Your proof of payment is to reach us before 5pm on the last day of the month to prevent service interruption on the 1st of each month.