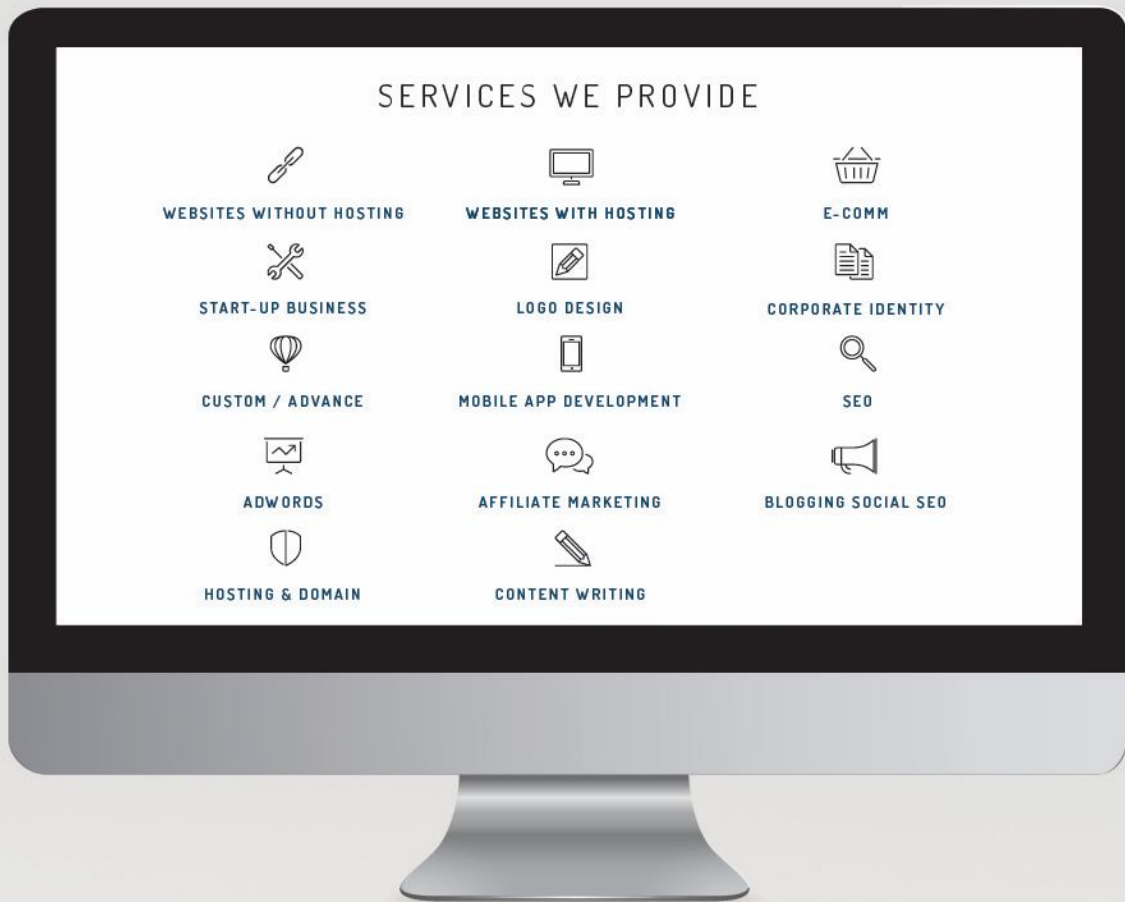
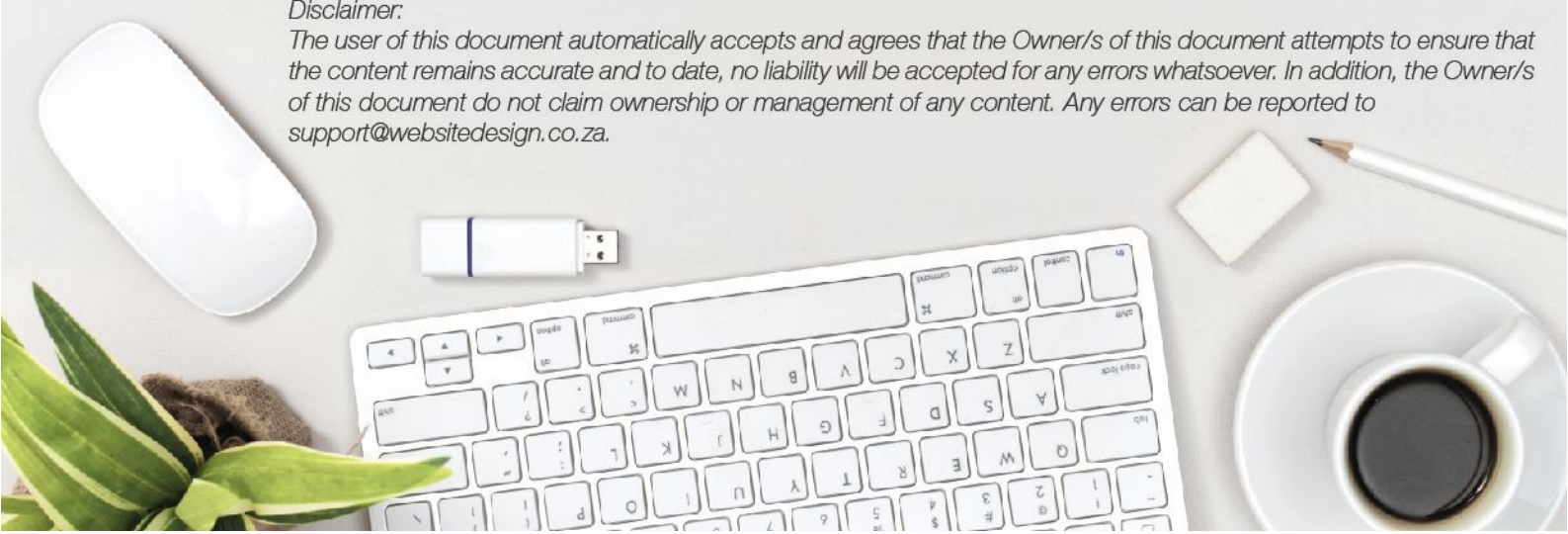


# Acceptable Usage Policy



**Disclaimer:**

The user of this document automatically accepts and agrees that the Owner/s of this document attempts to ensure that the content remains accurate and to date, no liability will be accepted for any errors whatsoever. In addition, the Owner/s of this document do not claim ownership or management of any content. Any errors can be reported to [support@websitedesign.co.za](mailto:support@websitedesign.co.za).



# Acceptable Usage Policy

---

## \*\*\* Contents Page \*\*\*

SPAM and Unsolicited Email .....	2
Offensive Content.....	4
Misuse of account features .....	5
Shared Systems and Resource Usage.....	5
Server Side processes.....	7
Internet Abuse.....	8
Security.....	9
Disk usage.....	10
Web Hosting Traffic Usage .....	11

## SPAM AND UNSOLICITED EMAIL

### 1. SPAM and Unsolicited Email

Last updated: March 2017

Sending unsolicited commercial communication (including, but not limited to email, instant messaging, SMS, chat rooms, discussion boards and newsgroups) is not permitted via Website Design's network.

Regardless of how the recipient's email address was acquired, if email communication was not explicitly requested or consented to by the recipient or if the recipient would not expect to receive it as a result of an existing relationship, the communication is considered unsolicited (this applies to communication sent to both personal email addresses and company email addresses e.g. sales@companyxyz.co.za). Email communication that does not clearly originate from a consensual sender or which appears to come from a 3rd party or affiliate is considered unsolicited.

Examples of unsolicited communication:

- Purchased mailing lists, "safe lists" and harvesting of email addresses, where the users of those email addresses have not explicitly agreed to receive communication from a specified consensual sender is considered unsolicited.
- Sending emails where the recipient must opt-out of receiving further emails that they didn't originally request is considered unsolicited.
- Sending a once-off invitation to receive further information, which was not explicitly requested or consented to by the recipient is considered unsolicited.
- Email communication to a mailing list including addresses of unwilling recipients or a recipient who has indicated that they wish to be removed from such list, yet continues to receive unwanted emails after a reasonable period, is considered unsolicited.

1.1 Mailing list operators should maintain meaningful records of recipient requests and their consent to receive said email communications. There should also be an option for the recipient to unsubscribe from receiving further email communications.

1.2 When Website Design receives a spam complaint, in order to establish if the communication was unsolicited, we may ask you to verify whether the recipient agreed to receive communications from you and if so, when and where you recorded their email address.

1.3 Website Design reserves the right to suspend or terminate the account of any user who sends out unsolicited email otherwise known as Spam with or without notice in accordance with its General Terms and Conditions.

As a Website Design customer, should you infringe this policy, you will be held liable for any costs incurred by Website Design, both monetary and in reputation. Website Design reserves the right to charge the customer of the account used to send any

unsolicited email a clean-up fee or any charges incurred for blacklist removal. This cost of the clean-up fee is entirely at the discretion of Website Design.

The use of any other service for the purposes of sending SPAM with any reference to Website Design services (including but not limited to mailboxes, autoresponders, and Web pages), will also be grounds for suspension/termination as described above. If your website was compromised and exploited for the purpose of sending unsolicited communications, Website Design will be more lenient in resolving the issue. However, repeat exploitations of the same website and/or customer account would be grounds for suspension/termination.

## OFFENSIVE CONTENT

Last updated: March 2017

2.1 Website Design does not allow any of the following content or links to such content, to be published on its Hosting Systems:

- 2.1.1 Content of a pornographic, sexually explicit or violent nature.
- 2.1.2 "Hate" sites or content that could be reasonably considered as discriminatory in any way including by way of sex, race or age discrimination.
- 2.1.3 Content of an illegal nature (including stolen copyrighted material).
- 2.1.4 Content that is defamatory or violates a person's privacy.
- 2.1.5 Content that involves theft, fraud, drug-trafficking, money laundering or terrorism.
- 2.1.6 Pirated software sites.
- 2.1.7 Illegal gambling sites.

2.2 If Website Design in its sole discretion determines that any customer content violates any law, including the Film and Publications Act, 65 of 1966 or this policy, it may:

- 2.2.1 Request the customer to immediately remove such content; and/or
- 2.2.2 Require the customer to modify such content; and/or
- 2.2.3 Without notice, suspend or terminate access to any services; and/or
- 2.2.4 Without notice, delete the offending content; and/or
- 2.2.5 Notify the relevant authorities of the existence of such content (if required by law or otherwise), make any backup, archive or other copies of such material as may be required by such authorities, disclose such elements of the customer's data as may be requested by the authorities and take such further steps as may be required by such authorities.

## **MISUSE OF ACCOUNT FEATURES**

Last updated: March 2017

3.1 Operating any service which makes an account feature available to third parties for any use other than normal access to that account's Web site is forbidden. Operating any service which enables or assists anonymous or abusive behaviour by third parties is forbidden. Operating any service which affects the stability or reliability of any Website Design server or network component, impacts other users or the company negatively, or degrades quality of service is forbidden. All account features are to be used solely in order to develop and implement the Web site(s) associated with that account.

3.2 Reselling Multiple Domains on Website Design's Web Hosting packages to a third party is not allowed. Multiple Domains are to be used solely for the Profile Owner's own websites.

## **SHARED SYSTEMS AND RESOURCE USAGE**

Last updated: March 2017

Customers hosting on our shared environment may not use any shared system provided by Website Design in a way that interferes with the normal operation of the shared system, or that consumes a disproportionate share of the system's resources. For example, excessive server hits, excessive bandwidth usage, excessive disk usage, inefficient scripts or database queries may compromise other users of the shared hosting environment. Website Design is authorised to suspend a user's account should it be found that excessive resource usage is negatively impacting on other customers of our shared hosting environment. In most cases, the examples below do not apply to Website Design Dedicated servers.

4.1 Users may not, through a cron job, CGI script, interactive command, or any other means, initiate the following on Website Design's shared servers:

4.1.1 Run any process that requires more than 50MB of memory space.

4.1.2 Run any program that requires more than 30 CPU seconds.

4.1.3 Run more than 10 simultaneous processes.

4.1.4 Send out mail to more than 500 recipients (email addresses) within one hour. 500 recipients represent one of the following: 500 recipients for one email, 500 individual emails or a combination of the two.

4.1.5 Send or receive, through mail, any file larger than 20MB.

4.2 Should we discover that a customer is performing bulk mail runs on our shared systems that exceeds the limit communicated in 4.1.4 above, regardless of whether it constitutes SPAM or not, Website Design will deactivate the user's account.

4.3 Custom server-side CGI scripts are to be run only by users with the appropriate package types (in Website Design's case the Web Hosting Basic package or higher). No user may run CGI scripts for the benefit of external sites or services. The use of system resource limits is intended to prevent runaway CGI scripts on an unattended

server. Also, processes with large memory footprints or hungry CPU requirements will incur swapping and other slowdowns that cause problems for every site on the server.

4.4 Interactive Web applications, commonly known as "chat", are not allowed on Website Design's shared systems. These applications are better placed on dedicated servers.

4.5 MySQL databases are provided to users of our web hosting packages:

4.5.1 Each qualifying individual package is limited to the allocated quota as published in the product matrix.

4.5.2 Each individual database is allotted a maximum of 500 MB disk space.

4.5.3 Databases may not be used for circumventing package disk allowances by storing web sites within the database.

4.5.4 Databases may only be used in conjunction with Website Design hosted packages. Access to databases from outside our local network is provided strictly for site and database development.

4.5.5 Only 10 concurrent MySQL connections per database user are allowed.

4.5.6 Databases may not be used to store binary files (including but not limited to image and application files). The database needs to reference the image on the user's site rather than actually storing the image i.e. these files should be stored within the user account and referred to in the database by using a link.

4.5.7 Website Design reserves the right to require changes to databases and database usage should they have an adverse impact on a database server and/or other user databases on that server. Website Design may move the database to a new server, or in extreme cases, Website Design reserves the right to disable any database determined to be harming performance of a database server.

4.6 The use of "cron jobs" (processes that are run automatically at certain times, in accordance with a "crontab" file set up by each user), are allowed on Website Design servers, subject to the following conditions and restrictions:

4.6.1 To be used only by customers of our web hosting packages

4.6.2 The job must not execute more often than every two hours.

4.6.3 If a cron job is likely to consume excessive CPU usage, it should be given a lower CPU priority.

4.7 Resource limits are enforced by automatic monitoring systems. This is not applicable to Fully Managed Dedicated servers, providing that it does not interfere with Website Design's ability to manage the server on the customer's behalf.

## **SERVER SIDE PROCESSES**

Last updated: March 2017

5.1 The installation or operation of any stand-alone, unattended server-side process (daemons) on Website Design servers, with the exception of cron jobs as per point 4 above, is not possible. Violation of this policy will result in immediate account termination without warning. This is not applicable to Website Design's Dedicated servers, providing that it does not interfere with Website Design's ability to manage the server on the customer's behalf.

5.2 This policy exists for several reasons:

5.2.1 To protect the CPU and memory resources available on each server.

5.2.2 To protect and enhance system security by not allowing unapproved third-party programs to accept connections from the outside world.



## INTERNET ABUSE

Last updated: March 2017

You may not use our network to engage in illegal, abusive, or irresponsible behaviour, including:

6.1 Unauthorised access to or use of data, services, systems or networks, including any attempt to probe, scan or test the vulnerability of a system or network or to break security or authentication measures without express authorisation of the owner of the system or network;

6.2 Monitoring data or traffic on any network or system without the authorisation of the owner of the system or network;

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

6.4 Use of an Internet account or computer without the owner's authorisation;

6.5 Collecting information by deceit, including, but not limited to Internet scamming (tricking other people into releasing their passwords), password robbery, phishing, security hole scanning, and port scanning;

6.6 Use of Website Design's service to distribute software that covertly gathers information about a user or covertly transmits information about the user;

6.7 Any activity or conduct that is likely to result in retaliation against our network;

6.8 Any activity or conduct that is likely to be in breach of any applicable laws, codes or regulations including the Electronic Communications and Transactions Act 25 of 2002 (see ECT Act) which renders you liable to a fine or imprisonment;

6.9 Introducing intentionally or knowingly into Website Design's service any virus or other contaminating program or fail to use an up to date virus-scanning program on all material downloaded from the Web;

6.10 Forging email or other messages is forbidden. Trafficking in pirated software is forbidden. Port scanning or the use of similar tools is forbidden.

6.11 Use of Website Design services to publish or otherwise disseminate information about the availability of pirated software or other material that is being made available illegally, including the publication of a list of links to such material, regardless of disclaimers, is specifically forbidden. We do not condone any illegal material or behaviour.

6.12 Should it be determined that the computers on your network have been infected with viruses or malware, you will be required to clean out the computers at your own cost. This is to prevent damage to the server's reputation and listing with blacklisting authorities. Failure to clean out the computers, may result in the deactivation of all services on your domain.

Compliance with the acceptable use policies of any network or system with which you connect through our service is required. If inappropriate activity is detected, all accounts of the user in question will be deactivated until the investigation is complete. Prior notification to the user is not assured. In extreme cases, law enforcement will be contacted regarding the activity.

## **SECURITY**

Last updated: March 2017

Website Design customers must take reasonable security precautions. Negligence could result in the hacking of websites as well as compromised mailboxes due to vulnerable PCs, website software or the use of weak passwords, which could affect other Website Design customers through blacklisting, phishing or spamming.

7.1 It is the customer's responsibility to ensure that scripts/programs installed under their account are secure (using the latest version) and permissions of directories are set properly, regardless of installation method. Users are ultimately responsible for all actions taken under their account. This includes the compromise of credentials such as user name and password. It is required that customers use a secure password. If a password is found to be weak, Website Design will notify the user and allow time for the user to change/update the password. Failure to make a password change that inadvertently leads to the website being compromised could result in the user's account being suspended / terminated.

7.2 Passwords should consist of at least 8 mixed alpha and numeric characters with case variations. Customers should not use a common word as a password and should change their passwords regularly. In the event of abuse Website Design reserves the right to reset a password.

## **DISK USAGE**

Last updated: March 2017

8.1 Accounts with many files can have an adverse effect on server performance. Website Design has the following limit: 100 000 files (i.e. an email, webpage, image file, folder etc.), or 25 000 files per folder. Accounts exceeding the above limit will have those files and/or folders excluded from our backup system.

8.2 Using our servers as a personal storage facility is not permitted. Any content stored must be directly related to the website(s) in question.

8.3 Mailboxes that build up large volumes of email without being accessed are not allowed (e.g. catchall mailboxes or bounce message mailboxes). The primary cause of excessive disk usage can be due to customers having their catchall address enabled, yet never checking their primary account mailbox. Over time, tens of thousands of messages build up, pushing the account past our file limit.

8.4 Email older than 6 months may not be stored on the server.

8.5 Individual emails that are 5MB or larger may not be stored on the server for more than 1 month.

8.6 Website Design has a disk usage quota in place for its Web Hosting packages. Where applicable, customers are sent monthly emails from Website Design notifying them of domains that have exceeded the allocated quota, providing an opportunity to reduce disk space or upgrade to a higher package in order to avoid unnecessary charges for over-usage. Customers can regularly monitor their disk usage via konsoleH by clicking on 'Disk Usage' under Statistics & Reports, which will give customers a reading of the total size of the package together with a summary of individual folder sizes.

8.7 In order for Website Design to operate with greater efficiencies and for our customers to have the flexibility and control of actively managing their disk space, an automated system tracks, notifies and charges for over-usage.

## WEB HOSTING TRAFFIC USAGE

Last updated: March 2017

9.1 Our Web Hosting packages have a set quota on the data transfer (traffic) for each domain. It is expected that all customers comply with this Acceptable Usage Policy, designed to preserve Website Design's server and network performance for the benefit of all our customers. Our Web Hosting packages are not suited to support the sustained demand of large enterprises; in such cases a dedicated server would be more appropriate.

9.2 Using a Web Hosting package primarily for online file storage or archiving electronic files is not permitted.

9.3 Streaming excessive video or hosting music on a Web Hosting package is prohibited.

9.4 Certain services may not be hosted on our dedicated servers & our Colocation offering without prior consultation. Examples include, but are not limited to:

1. Public mirroring services that are made available for general public use
2. Any website or service where the primary focus is to drive or redirect traffic from one network to another
3. Reselling bandwidth and/or network capacity as internet access to end users