

**Johannesburg:** Tel. 011-803 2316 Fax 011-803 2022  
Camsoft, 40 Eighth Avenue, Woodmead Extension, 2146  
PO Box 36303, Glosderry, 7702

**Cape Town:** Tel. 021-797 4845 Fax 021-797 4744  
Camsoft House, 40 Bayview Road, Wynberg, 7800

[www.camsoft.co.za](http://www.camsoft.co.za) • [info@camsoft.co.za](mailto:info@camsoft.co.za)



## **AUP (Acceptable Usage Policy)**

Revision 1.05

This Acceptable Use Policy ("AUP") is intended to enhance the use of the computing resources and Internet usage at Camsoft by promoting lawful and acceptable use and preventing unacceptable use. This document also specifies the actions prohibited to users of the network and systems ("infrastructure") of Camsoft and details how users are required to adhere to all the policies specified in this AUP without exception.

### **Laws and Regulations**

1. Camsoft's infrastructure may only be used for lawful purposes. Users may not violate any applicable laws or regulations of South Africa within the territory of South Africa.
2. Transmission, distribution or storage of any material on or through the infrastructure in violation of any applicable law or regulation is prohibited. This includes, without limitation, material protected by copyright, trademark, trade secret or other intellectual property right used without proper authorisation, as well as material that is obscene, defamatory, constitutes an illegal threat, or violates export control laws.
3. Camsoft's computer and Internet resources, including e-mail access, are for business use and may not be used for private use unless express permission has been granted by management subsequent to a staff member's specific request.

### **The Network**

1. The user acknowledges that Camsoft is unable to exercise control over the content of the information passing over the infrastructure and the Internet, including any websites, electronic mail transmissions, news groups or other material created or accessible over its infrastructure. Therefore, Camsoft is not responsible for the content of any messages or other information transmitted over its infrastructure.
2. Camsoft's infrastructure may be used to link into other networks worldwide and the user agrees to conform to the acceptable use policies of these networks.
3. The user may obtain and download any materials marked as available for download off the Internet but is not permitted to use its Internet access to distribute any copyrighted materials unless permission for such distribution is granted to the user by the owner of the materials.
4. The user is prohibited from obtaining and/or disseminating online any unlawful materials, including but not limited to stolen intellectual property, child pornography, and/or any unlawful hate-speech or racially prejudiced materials.
5. Staff members are prohibited from disseminating information on money-making schemes, chain letters, commercial advertising and informational announcements without the express permission of Camsoft's management.

## System and Network Security

1. The user may not circumvent user authentication or security of any host, network, or account (referred to as "cracking" or "hacking"), nor interfere with service to any user, host, or network (referred to as "denial of service attacks").
2. Violations of system or network security by the user are prohibited, and may result in civil or criminal liability. Camsoft will investigate incidents involving such violations and will involve and will co-operate with law enforcement officials if a criminal violation is suspected. Examples of system or network security violations include, without limitation, the following:
  - (i) Unauthorised access to or use of data, systems or networks, including any attempt to probe, snoop, scan or test the vulnerability of any system or network or to breach security or authentication measures without the express authorisation of Camsoft;
  - (ii) Unauthorised monitoring of data or traffic on the network or systems without express authorisation of Camsoft;
  - (iii) Interference with service to any user, host or network including, without limitation, mailbombing, flaming, flooding, deliberate attempts to overload a system and broadcast attacks;
  - (iv) Forging of any TCP-IP packet header (spoofing) or any part of the header information in an e-mail newsgroup posting.
  - (v) Utilising Denial of Service attacks, Trojans, e-mail worms or viruses to disrupt any other computing device either within the company or external to the company.
  - (vi) Installing file sharing/swopping software on any PC (whether for gaming, music sharing or otherwise) is strictly prohibited.
3. All references to systems and networks under this section include the Internet (and all those systems and/or networks to which user is granted access through Camsoft) and includes but is not limited to the infrastructure of Camsoft itself.
4. Staff members are not permitted to actively interfere with other staff members' computer equipment without the express permission of the affected staff member concerned or Camsoft management.
5. Content residing on Camsoft's computer systems may not be replicated onto any other media, including CDs, floppy disks or other back-up devices, or transferred out of the business via electronic means of any form, including e-mail and FTP other than for business use when and where necessary in the normal operation of the business.
6. All conditions, procedures and restrictions contained in Camsoft's Acceptable Usage Policy (AUP) are also applicable to staff members when on-site at a client's premises and where the client specifically requests the staff member to adhere to their own company's AUP the staff member should request a copy of this AUP prior to agreeing to any terms and conditions that it might contain.

## Data Protection and e-mail usage

1. It is explicitly prohibited to send unsolicited bulk mail messages ("junk mail" or "spam") of any kind (including and without limitation: "Make-Money-Fast" and pyramid schemes, commercial advertising, political tracts, announcements, virus warnings or hoaxes, etc). This is strongly objected to by most Internet users and the repercussions against the offending party and Camsoft can often result in disruption of service to other users connected to Camsoft. Camsoft distributes electronic news letters and promotional information to clients and prospects from time to time and when this occurs a specific request will be made by Camsoft's management for this activity to take place.
2. Maintaining of mailing lists by Camsoft's staff members is accepted only 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.

3. Staff members may not forward or propagate chain letters, virus warnings (either hoaxes or genuine warnings), nor malicious e-mail. A staff member is permitted and encouraged to advise individual senders of virus infected e-mail messages that they have become infected by a virus but only if the staff member's anti-virus software has been updated with the latest virus signature files.
4. It is the individual staff member's responsibility to ensure that their computing device is operating satisfactorily at all times and to make technical support staff aware of any malfunctioning hardware or software at their earliest convenience. Should a malfunctioning device or software not be rendered functional by the individual staff member or a technical staff member within a week of the malfunction being reported then the staff member is required to alert management of the status of the malfunction at this time.
5. It is the individual staff member's responsibility to ensure that their anti-virus software is being updated for virus signatures on a regular basis (i.e. at least weekly) and should this not be occurring a technical support staff member should be notified and failing the rectification of this problem after more than 1 week the staff member should immediately notify management .
6. No profane, abusive or impolite language should be used in e-mail communications.
7. Camsoft reserves the right to examine staff members' mail folders and Internet access logs to confirm that no mails sent or Internet usage are in contravention of Camsoft's Acceptable Usage Policy or should the need arise due to a complaint by a third party. Camsoft also reserves the right to examine the mail servers of any users using Camsoft's mail servers for "smarthosting" (when the user relays its mail off a Camsoft 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 Camsoft's policy of preserving customer privacy.
8. Staff members are required to ensure that important company data resides only on the Camsoft Server in the local office and should work need to be taken home or off-site for whatever reason it needs to be protected against compromise in the case of theft by file encryption software provided by Camsoft. Such data should also be backed up to a server-based copy when returning to the office if changes have been made to the data while out of the office. Staff members are also required to ensure that their individual e-mail folders, i.e. pst files for Outlook and the like, are backed up to the server at least once a week should these folders reside on their local workstations.
9. The onus is on the staff member to whenever possible ensure that their own computing device supplied by Camsoft is not compromised by any other third party, including but not exclusively usage by other staff members, spouses, relatives and friends. Staff members are permitted to make use of computing devices of other staff members only with the express permission of the staff member whose computing device is to be used. Camsoft supplies personal firewall software that should be installed and maintained on every staff member's PC.
10. Staff members are prohibited from using any company domain names, such as those in their business e-mail addresses, to correspond with any third party, submit or request information or join news/chat groups and the like, in such a manner that will bring the company into disrepute in any way.
11. The downloading and transmission of MP3, VCD, MPEG, DVD or other format music or video files, as well as files for non-business use other than those specifically granted permission for by management is not permitted using company Internet, FTP or e-mail access resources.
12. The individual staff member is required to ensure that sufficient password protection is provided on their own computing device and all passwords without exception are to be provided to the staff member's manager for safe keeping. Should a staff member change their passwords in any way the new passwords are to immediately be provided to their business manager. Passwords are to be treated as strictly confidential and every endeavour needs to be made to ensure that they are not compromised by any third party.
13. Employees using mobile devices containing company information such as customer records and notes, fields, sales information and contact details relating to customers must ensure that adequate security is in place on the device at all times with strong password protection. At no time should such devices be lent or sold to any 3<sup>rd</sup> party not directly in the employ of Camsoft without the express permission of Camsoft and prior to such data being removed.

## **Web Site Access**

1. Staff members are not permitted to willingly access or download undesirable content of any form, including but not exclusively content that contains in image, text or video format pornography, racial prejudice, violence, sexism or hate-speech from the Internet or other resources. This restricted content is also not permitted to be stored on any media whatsoever in Camssoft's offices.
2. Staff members may not visit any pornographic or other undesirable Web sites. If they happen upon such a site by chance, they must leave it immediately, before exploring it.
3. Users may not play computer-based games of any kind, including Web-based games, in Camssoft offices at any time and games are not permitted to be downloaded via http, ftp or other means using Camssoft's computer equipment and/or Internet access. Computer games of any kind are also not permitted to be transmitted via e-mail or any other means from Camssoft's offices to any other user either within the business or to a third party outside of the business.
4. Chat lines may not be accessed from the workplace other than those specifically used for business purposes.
5. Clients' data such as databases and e-mail folders are to be treated with the same security provisions as Camssoft's data and under no circumstances whatsoever permitted to be distributed to any unauthorised third parties outside of the business.
6. Staff members who visit undesirable sites, play games on the Web, download, create or print unsuitable material, behave inappropriately or infringe any of the above conditions for appropriate usage, may be banned from using the Internet facilities for varying periods of time. In the case of regular infringements, further disciplinary action will be taken.
7. All content, including e-mails, databases, spreadsheets, documents and images on computer equipment owned by Camssoft is deemed to be the property of Camssoft and as such can be scrutinised at any time by management without forewarning. All such content should also comply with the provisions provided by Camssoft's Acceptable Usage Policy and it is the individual user's responsibility that this is enforced on the computer equipment assigned to their individual use, or if a server device has been assigned to their responsibility, on this device as well.

## **Supplier Portals & Usenet News**

1. Users are expected to use supplier portals responsibly and at all times exhibit acceptable respect towards others making use of the portal, including refraining from abusive language, unnecessary criticism, racial, sexual or hate speech remarks.
2. Users are not permitted to make derogatory remarks about Camssoft, its clients or suppliers on any Portals, newsgroups or in any other public forum, electronic, print or otherwise.
3. Excessive cross-posting (i.e. posting the same article to a large numbers of newsgroups) is forbidden.
4. Posting of irrelevant (off-topic) material to newsgroups (also known as USENET spam) is forbidden.
5. Posting binaries to a non-binary newsgroup is forbidden.
6. Camssoft reserves the right to delete and/or cancel posts which violate the above conditions.

## Social Networking Services and Video sharing sites

1. Employees of Camsoft are not permitted to create identities or profiles using Camsoft's, its clients or suppliers names or brands in any form whatsoever on social networking sites including but not restricted to sites such as Twitter, Facebook,, MySpace, without the express written permission by management at Camsoft to do so.
2. Employees are not permitted to access any social networking services of any kind for personal use whilst at work or using company electronic equipment and bandwidth resources.
3. Employees of Camsoft are not permitted to create movies or still images of any kind whatsoever using Camsoft, its clients or suppliers' names or brands in any form on either social networking sites or video sharing sites, including but not restricted to sites such as UTube and MySpace, without the express written permission by management at Camsoft to do so.
4. Employees are not permitted to access any video sharing sites, including but not restricted to sites such as UTube and MySpace for personal use whilst at work or using company electronic equipment and bandwidth resources.
5. Users are not permitted to make derogatory remarks about Camsoft, its clients or suppliers' on any social networking sites or video sharing sites of any description at any time during or after work hours.

## Complaints

Upon receipt of a complaint, or having become aware of an incident, Camsoft reserves the right to:

- (i) Inform the staff member's manager of the incident and require the manager to deal with the incident according to this AUP;
- (ii) In the case of individual staff members suspend the staff member's account and withdraw the staff member's network access privileges completely;
- (iii) In severe cases suspend access of the staff member's entire network until abuse can be prevented by appropriate means;
- (iv) Share information concerning the incident with other Internet access providers, or publish the information, and/or make available the staff member's details to law enforcement agencies.
- (v) Any one or more of the steps listed above, insofar as they are deemed necessary by Camsoft in its absolute and sole discretion, may be taken by Camsoft against the offending party.