HELDERBERG COLLEGE OF HIGHER EDUCATION
COMPUTER AND ELECTRONIC SERVICES ACCEPTABLE USE POLICY
29 December, 2004

1. PURPOSE:
To set policy for the use of the College's electronic information systems, including users' rights and responsibilities.

2. APPLICABILITY:
This policy applies to all individuals accessing and using computing, networking, telephony and information resources through any facility of Helderberg College. These individuals include students, any staff (including visiting staff), volunteers, alumni, persons hired or retained to perform College work, external individuals and organisations, and any other person extended access and user privileges by the College under contractual agreements and obligations or otherwise.
This policy covers all computing, networking, telephony and information resources owned by, procured through, operated or contracted by Helderberg College. Such resources include computing and networking systems (especially those connected to the College's telecommunications infrastructure), public access sites, shared computer systems, personal desktop computers, other computer hardware, software, and databases stored on or accessible through the network.

3. ACCOUNTABILITY:
Under the President of Helderberg College, the Vice President for Academic Affairs and the Director for the Computer Services Department (CSD) shall ensure compliance with this policy. The Dormitory Deans, President, Vice Presidents, Computer Services staff, Student affairs staff, and individual Heads of Department shall implement the policy.

4. GENERAL PRINCIPLES:
4.1. The College owns its computing, networking, telephony and other communications systems and its information resources, and has the right to monitor them. The College also has various rights to the software and information residing on, developed on, or licensed for these computers and networks. The College has the responsibility for the security, integrity, maintenance and confidentiality of the electronic systems.

4.2. Computing, networking, telephony and information resources of the College, exist to support students and staff as they carry out the education, research and public-service missions of the College, and its management. Toward these ends, the College encourages and promotes the use of these resources by the College community. Access to and use of these resources for purposes or activities which do not support the College's missions are subject to regulation and restriction to ensure that they do not interfere with legitimate work; and any access to or use of these resources and services that interferes with the College's missions and goals is prohibited.

4.3. When demand for computing, networking, telephony and information resources exceeds available capacity or resources, priorities shall be established for allocating the resources, with a higher priority to activities essential to the missions of the College. The President and Vice Presidents, in conjunction with the Computer Services Department (CSD), shall set these priorities.

4.4. The CSD, shall develop and publicise specific written procedures to protect the rights of legitimate authorised users, to protect the integrity of the information and systems under their management, and to delineate the responsibilities of users. The CSD has the authority to control or refuse access to anyone who violates these procedures or threatens the rights of other users or the availability and integrity of the systems and the information. Actions that may be taken under this
authority include deactivating accounts, access codes or security clearances; stopping processes; deleting affected files; and disabling access to computing, networking, telephony and information resources.

4.5. Users' expectation of electronic privacy must be balanced against the College's reasonable need to supervise, control and operate the College's information systems.

5. RIGHTS OF THE USER:

5.1. *Privacy and confidentiality:* Because the primary use of the College's communications systems is to further the College's mission, members of the College community should not have the expectation of privacy in their communications, whether work related or personal. By their nature, electronic communications, especially E-mail connected to the Internet, may not be secure from unauthorised access, viewing or infringement. Although the College employs technologies to secure certain categories of electronic messages, as a rule confidentiality of E-mail and other electronic documents cannot be assumed. The College cannot and does not make any guarantee, explicit or implied, regarding the confidentiality of E-mail and other documents and messages stored in electronic media unless provisions, approved and maintained by the College, are specifically implemented to this purpose. Users should not expect total privacy when using E-mail.

Although the CSD will *not* monitor the content of electronic documents or messages as a routine matter, it reserves the right to examine all computer files in order to protect individuals and the College. In addition, during the course of routine conduct of College business, routine management of the College's computing and networking systems, as well as during emergencies, the CSD has the right to view or monitor users' files, data, messages or other activity for legitimate business purposes, with or without notice to users. Information seen in such a manner will ordinarily be kept confidential, but may under certain circumstances be used in disciplinary proceedings if appropriate. If an individual is suspected of violations of his/her responsibilities as described in this policy or of other misconduct, the College reserves the right to take any and all actions to abide by the law and maintain network integrity and the rights of access of others authorised to use the system. The College also reserves the right to access and disclose messages, data, files, and E-mail back-up or archives, if such exist, to law enforcement authorities and others as required by law, to respond to legal processes, and to fulfil its obligations to third parties.
Therefore, good judgment dictates the creation only of electronic documents that may become public without embarrassment or harm. It must be noted that any email messages left in a user's inbox on the Email Server are encrypted, and any attempt to decipher the contents for general perusal would be virtually impossible. Thus, email within a server mailbox can only be accessed through a legitimate account name and password.

5.2. *Safety:* Unwanted communications and offensive or objectionable materials are available through the Internet and may be blocked or regulated by the CSD. The College or CSD accepts no responsibility for the content of electronic mail received. However, threatening, harassing or offensive communications received by College personnel over the network should be reported to the CSD.

5.3. *Intellectual freedom:* The network is a free and open forum for the expression of ideas. The CSD will not prevent expressions of academic opinions on the network as long as these opinions are not represented as the views of the College and are not in conflict with College policies. Even with disclaimers about not representing the views of the College, appropriate language, behaviour and style should still be used in communications distributed on the College's computing and networking facilities. It should be remembered that certain categories of speech, such as defamation, obscenity and incitement to lawlessness, are not protected by College policy. The CSD
reserves the right, at its sole discretion, to decline to post, to remove posted pages or to restrict College web sites or computer accounts which contain or are used for personal expressions of a non-academic nature.

6. GENERAL RESPONSIBILITIES OF USERS:

6.1. Individuals with access to the College's computing, networking, telephony and information resources have the responsibility to use them in a professional, ethical and legal manner. Users are required to take reasonable and necessary measures to safeguard the operating integrity of the systems and their accessibility by others, while acting in a manner to maintain an academic and work environment conducive to carrying out the College's mission efficiently and productively. Specifically, responsibilities of users include:

6.1.1. Respecting the rights of others, including intellectual property, privacy, freedom from harassment, and academic freedom;
6.1.2. Safeguarding the confidentiality of certain information and the privacy of the College community;
6.1.3. Using systems and resources so as not to interfere with or disrupt their normal opera tions or their access use and use by others so authorised;
6.1.4. Protecting the security of College electronic systems and the integrity of information stored there;

6.2. Individuals are prohibited from sharing passwords or log-in IDs or otherwise giving others access to any system for which they are not the data stewards or system administrators with appropriate authority. Users are responsible for any activity conducted with their computer (or other device) accounts and are responsible for the security of their passwords. Only authorised persons may use the College's electronic communications systems. Spouses, and other family members of authorised persons must have prior permission from the CSD, or appropriate department depending on equipment (for example, Finance Department for use of Photostat machines). The CSD or the appropriate department has the right to deny access, and it is the responsibility of the user to seek out the correct department in which to gain permission.

6.3. Individuals may not use another person's network account or try to obtain password or access code to another's network account to send or receive messages. If this does occur, the CSD must be given prior notice, and will either allow or deny this generally discouraged activity.

6.4. Individuals must identify themselves and their affiliation accurately and appropriately in electronic communications and may not disguise the identity of the network account assigned to them or represent themselves as someone else.

6.5. The College's communications systems may not be used to harass, intimidate, threaten or insult others; to interfere with another's work or education; to create an intimidating, hostile or offensive working or learning environment; or to conduct illegal or unethical activities.

6.6. The College's networks may not be used to gain or attempt to gain unauthorised access to remote networks or computer systems.

6.7. Individuals are prohibited from deliberately disrupting the normal operations of the College's computers, workstations, terminals, peripherals or networks.

6.8. Individuals may not run or install on any College computer system a program that may result in intentional damage to a file, or that may intentionally compromise the integrity of the College's systems or the integrity of other computing environments via the College's network (e.g., computer viruses, Trojan horses, worms, key loggers, or other rogue programs). Users may also not store information that may lead to the compromising of the College network (e.g., Hacking documents).

6.9. Individuals are prohibited from circumventing access and user authentication systems, data-protection mechanisms, or other security safeguards.

6.10. Individuals must abide by all applicable copyright laws and licenses, and respect other intellectual property rights. Information and software accessible on the Internet is subject to copyright or other intellectual property right protection. College policy and the law forbid the unauthorised copying of software that has not been placed in the public domain and distributed as "freeware." Therefore nothing should be downloaded or copied from the Internet for use within the College unless express permission to do so is stated by or received from the owner of the material, and the owner's requirements or limitations on use of the material are observed. The use of software on more than the licensed number of computers, unauthorised installation of unlicensed software on College computers, plagiarism and invasion of privacy are also prohibited. "Shareware" users must abide by the requirements of the shareware agreement.

6.11. Activities that waste or unfairly monopolise computing resources, such as unauthorised mass mailings; electronic chain letters, junk mail and other types of broadcast messages; unnecessary multiple processes, output or traffic; exceeding network directory space limitations; excessive game playing or other trivial applications; and excessive printing, are prohibited.

6.12. Reading, copying, changing or deleting programs or files that belong to another person or to the College without permission is prohibited.

6.13. The College's computing resources may not be used for commercial purposes. Limited personal financial gain may be accepted if it facilitates a better College environment and does not contravene College policy. Permission must be obtained from the CSD.

6.14. All network communications exiting the College are subject to the acceptable use policies of the network through which they flow.

6.15. Use of the College's systems that violates local, state or national laws or regulations or College policies, standards of conduct, or guidelines is prohibited.

6.16. All computers or devices that could potentially harbour malicious programming code (eg. Viruses), must contain an updated antivirus application. Contact the CSD for further information.

7. E-MAIL AND OTHER ELECTRONIC COMMUNICATIONS

This includes, but is not limited to Email, Internet services, Voice mail, Audio and Video Conferencing, and Facsimile messages:

7.1. The use of College resources for electronic communications must be related to College business, including academic pursuits, and not for personal or commercial purposes, except for incidental and occasional personal non-commercial use when such use is clearly insignificant, does not generate a direct cost for the College, and does not interfere with or compete with legitimate College business.

7.2. Electronic communications whose meaning, transmission or distribution is illegal, unethical, fraudulent, defamatory, harassing or irresponsible are prohibited. Material that may be considered inappropriate, offensive or disrespectful to others should not be sent or received as electronic communications using College facilities.

7.3. Appropriate standards of civility and decency should be observed in electronic (as well as all other forms of communication.

7.4. Email accounts are supplied to registered students and staff free of charge. Application forms are available from the CSD.

8. HELDERBERG COLLEGE WEB PAGE:

8.1 "Official" College Web pages are those that provide information about established, College recognised entities, such as its faculties, administrative offices, centres, and educational programs. Information on official College Web pages represents the institution and therefore must be accurate, timely and useful and must conform to College policies, standards and requirements. Official Web pages shall be held to the same standards as any College, school or unit printed publication.

8.2. The Computer Services Director is responsible for official web pages. This individual or his/her designees (such as the webmaster) must authorise the establishment of any official web page under their purview.

8.3. The College logo must appear on all official web pages, or their equivalent.

8.4. Official web pages shall be reviewed by the responsible party at least every six to twelve months. Pages requiring frequent updating, must be reviewed the day they are published.

8.5. Official web pages may be copyrighted. Official pages should not contain copyrighted materials without appropriate copyright permission. Policy related information must be approved through relevant committees before it is published.

8.6. Official web pages should be created with similar or consistent themes (e.g., font, spacing, colours).

9. FACULTY AND PERSONAL WEB PAGES:

9.1. Web pages may not promote illegal activities; harass anyone inside or outside the College; include offensive or objectionable material or language or link to other sites that do; distribute copyrighted materials; be used for commercial purposes or personal gain unrelated to the College's mission.

9.2. Pages may not contain the College logo or represent the contents as being the official policy or positions of the College.

9.3. Personal web pages must include the identity of the author, and should contain the following statement: "The contents, views and opinions expressed in this page are strictly those of the author and not necessarily of Helderberg College." The CSD reserves the right to not post or remove posted pages for any reason.

9.4. Personal Web pages contain "hbc.ac.za" as part of their URLs, and therefore reflect the Author's affiliation with Helderberg College. Therefore, they should not contain material that undermines Helderberg College's statement of purpose and its character as a church affiliated institution. This includes material that is highly offensive, profane, vulgar or abusive.

9.5. Personal Web pages must not contain illegal material. This includes text, images, music or programs that are copyrighted by other people unless the copyright owner has given written permission for their use on the World Wide Web.

9.6. Pages maintained on a College server or in the domain "hbc.ac.za" must not contain direct links to sites which contain materials that threaten, harass, intimidate, are obscene, or violate copyright, patent protections, license agreements and other intellectual property rights, the College's code of conduct, or College rules or policies.

9.7. Authors of Web documents and those who store resources on College servers are solely responsible for their content.

9.8. Web pages should not be listed with sites or appear in messages of sites that are associated with some form of net abuse, illegal activity, or violation of College policies. This will be treated as a violation of this policy.

9.9. Personal web pages are a shared resource. Therefore, it is not an appropriate place to offer any services, commercial or not, that is likely to attract a large volume of network traffic from the Internet or intranet as a whole.

9.10. User written CGI programs are not supported. Any kind of server side scripting language poses security risks, and the CSD reserves the right to allow or disallow this generally discouraged activity.

9.11. Personal web pages must be housed on a Helderberg College web server, and only registered College students and staff may make use of this facility. The disk usage limit is 15 Megabytes.

9.12. Contact the CSD for an application form.

10. COMPUTER SOFTWARE AND HARDWARE STANDARDS

10.1. *Software Standards*

So as to maintain a high level of quality on campus, all computers are installed with software to meet with particular requirements:

10.1.1. The need they must fulfil;
10.1.2. Current industry standard.

10.2. *Hardware Standards*
The campus computers are divided into 3 groups: the computers in the Computer Laboratories (for students), the Staff Computers, and the Servers (which provide particular services and resources to the campus community).
So as to maintain a high level of quality, all new computers are acquired taking into account certain requirements:

10.2.1. The need they must fulfil;
10.2.2. Current industry standard.

NON COMPLIANCE AND SANCTIONS:
Infractions must be reported the Computer Services Department.
Non compliance with the electronic communications policy, the CSD, may at their discretion, and without notice, deny or remove access privileges to the College's electronic systems. This includes cutting off web access to pages generating excessive traffic which impacts system/network performance or service to other users.

Disciplinary action under applicable College policies and procedures, civil litigation, and/or criminal prosecution under applicable national and/or international laws may also occur.