NETWORK AND COMPUTER USE POLICY

I. PURPOSE:

This policy governs the use and operation of Cheyney University 's Information Technology (IT) resources and services (computers, printers, data networks, and any other current or future Information Technology (IT) resources adopted by the university). This policy applies to Information Technology (IT) resources in offices, classrooms, labs, residence halls, etc. both on-campus and off-campus. The intent of the policy is to provide a productive work environment and to permit maximum use of Cheyney University 's Information Technology (IT) resources for academic, administrative, and student computing. Use of these resources is a privilege, not a right and is granted solely to Cheyney University faculty, staff and students. These privileges also apply to visitors, interim and temporary staff who use University Information Technology (IT) resources in any manner.

All Information Technology (IT) resources should be used for University-related business (instruction, research, academic and administrative activities). Users of these resources are expected to conduct their activities in a professional and responsible manner and follow the guidelines, restrictions and overall university policies of Cheyney University , the State System of Higher Education, the laws of the Commonwealth of Pennsylvania , and federal statutes.

II. POLICY:

As an institution committed to the principle that a quality education is the cornerstone of a democratic society, Cheyney University strongly encourages the free exchange of ideas and information among all members of its community and with members of other communities. The instruments of communication can stimulate intellectual, social, cultural, and emotional growth but they also can be a means to destroy and harass. Therefore, students, faculty and staff in the University community are expected to exercise responsibility, use computing resources ethically, respect the rights and privacy of others, and operate within the bounds of the law and of University policies and codes of conduct.

Improper use of Cheyney University 's Information Technology (IT) resources include (but are not limited to) the following:

1. Use of University Information Technology (IT) resources must comply with State and Federal Law, State System of Higher Education policies and University policies. Therefore, University Information Technology (IT) resources may not be used for commercial or profit-making purposes, for political purposes, or for personal benefit where such use incurs a cost to the University and is not academic or work related. Use of the University's microcomputers, workstations, or information networks must be related to a Cheyney University business. If the non-business usage of information services results in a direct cost to the University for any reason, it is the individual's responsibility to reimburse the university.
2. Users should only use the computer, network id and password assigned to them. Access of or attempts to access another person's computer, directories, files, or data communications whether protected or not are prohibited. Attempts to access unauthorized Information Technology (IT) resources via the computer network, to decrypt encrypted materials, or to obtain privileges to which the user is not entitled are prohibited. Sharing of a computer account with other persons is prohibited; User ids and passwords must be protected, and the user must not leave a machine logged on when the user is not present.
3. Theft, damage or destruction of computing equipment, facilities, programs or data is prohibited.
4. Information or software cannot be placed on any University owned computer system. Cheyney University has signed software licenses for much of the software that are available on the

computer systems; removal or transfer of such software without authorization is prohibited. All persons shall abide by the terms of all software licensing agreements and copyright laws.

5. Copying of site licensed software for distribution to persons other than Cheyney University faculty, staff, and students, or the copying of site licensed software for use at locations not covered under the terms of the license agreement, are prohibited.
6. Users of University Information Technology (IT) resources shall not consume unreasonable amounts of these resources. The University may impose restrictions or limits on use of such resources. Deliberate acts which are wasteful of computing\information network resources or which unfairly monopolize resources to the exclusion of others are prohibited. These acts include, but are not limited to, playing internet games, videos, MP3's, sending mass emails or chain letters, creating unnecessary multiple jobs or processes, obtaining unnecessary output, or printing or creating unnecessary network traffic. Any network traffic exiting the University is subject to the acceptable use policies of the network through which it flows (PREPnet, NSFNET, SSHEnet, etc.), as well as to the policies listed here.
7. Printing multiple copies of any document including handouts or announcements is also prohibited.
8. No person shall use IT resources to harass others; to send obscene mesages or materials; to threaten the safety of another; to send libelous messages or to interfere with the work of the University.
9. No person shall post materials on electronic bulletin boards that violate existing laws or the University's policies and codes of conduct.
10. The University may have a business necessity or reason to access files and accounts of its employees or students, including the investigation of complaints of misuse of the system. It is therefore unreasonable for any IT user to have an expectation of privacy in the use of Information Technology (IT) resources.
11. All other unauthorized acts or uses of university computing facilities or resources, or any other actions not in accordance with university policies, or not in the best interests of Cheyney University are prohibited.

III. **DISCIPLINARY CONSEQUENCES:**

The University reserves the right to limit or restrict computing\network privileges to its IT resources. Depending on the seriousness of an offense, violation of the policy can result in penalties ranging from reprimand, referral to University authorities for disciplinary action, to criminal prosecution. Misuse and\or abuse of these resources may result in the immediate removal of privileges pending final resolution.

Potential violators may also be subject to criminal prosecution under federal or state law, and should expect the University to pursue such action. As an example, under Pennsylvania law, it is a felony punishable by a fine up to $15,000 and imprisonment up to seven years for any person to access, alter or damage any computer system, network, software or database, or any part thereof, with the intent to interrupt the normal functioning of an organization [18 Pa.C.S. §7612]. Disclosing a password to a computer system, network, etc., knowingly and without authorization, is a misdemeanor punishable by a fine of up to $10,000 and imprisonment of up to five years, as is intentional and unauthorized access to a computer, interference with the operation of a computer or network, or alteration of computer software [18 Pa.C.S. §7611(a)(2) and (3)].