Cheyney University Policy FA – 2010-4030

Policy on Acceptable Usage of Technology

Approved by:	Finance and Administration Council/President's Cabinet
History:	Issued - 2-17-2009
	Revised -10-02-2013 FA Council; 02-11-14 President's Cabinet
Related Policies:	N/A
Additional References:	N/A

A. Purpose

Cheyney University promotes courteous, ethical and responsible use of all its Information Technology (IT) resources and services including but not limited to: computers, printers, video conferencing, telephones, cable TV, voice and video networks and outside networks where the university provides access and any other current or future Information Technology (IT) resources adopted by the university. This policy applies to the Information Technology (IT) resources in offices, classrooms, labs, residence halls, etc. both on-campus and off-campus, all electronic media, including but not limited to: campus and State System of Higher Education networks and systems, electronic mail, listserv and mailing lists, discussion groups, social networks, Internet and World Wide Web access, electronic records.

The intent of the policy is to if I had 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, into rum and temporary staff will use university Information Technology (IT) resources in any manner.

B. Scope

All Cheyney University faculty, staff, students, and visitors.

C. Definitions

No specialized definitions.

D. Policy

Cheyney University strongly encourages the free exchange of ideas and information among all members of its university community and with members of other communities. Information

Technology resources can stimulate intellectual, social, cultural, any motion of growth but they also can be a means to destroy and harass. Therefore, students, faculty and staff and 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. While the university recognizes the role of privacy there should be no expectation of privacy of information stored on or sent through university-owned information technology resources, except as required by state or federal law. The university may be required to provide information stored in its information technology resources to someone other than a user as a result of a court order, investigatory process, or in response to a request authorized under Pennsylvania's Right-To-Know statue (65 P.S. §67.101 et seq.).

Cheyney University's Information Technology (IT) Acceptable Use Policy includes (but is not limited to) the following:

I. <u>Responsibilities</u>

1. Respect to intellectual property of authors, contributors, and publishers in all media.
2. Report lost or stolen devices, including devices that contain private or university information, to Information Technology Services (IT) within 24 hours of discovery of loss;
3. Adhere to the terms of software licenses and other contracts. Persons loading software on any university computer must adhere to all licensing requirements for the software. Except where allowed by the university site licenses, copying for university use for personal use is a violation of this policy;
4. Adherence to all of the applicable university policies in terms of any collective bargaining agreement;
5. To use the university information technology resources in a manner that complies with state and Federal law.
6. User accounts – all Cheyney University faculty, staff and students are issued network and computer accounts. The following practices should be followed when using university use their accounts:

    a) Users should only use the computer, network ID and password assigned to them
    b) Access of or attempts to access another person's computer, directories, files, or data communications whether protected or not are prohibited
    c) 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 or prohibited
    d) Sharing of a computer account with other purses is prohibited;
    e) User IDs and passwords must be protected, and the user must not leave a machine logged on when the user is not present
    f) All faculty, staff and students are responsible for the security of his or her passwords. This includes changing passwords on a regular basis and properly securing them.

7. Email – all Cheyney University faculty, staff and students or issued an email account. The use of university e-mail is a privilege and maybe revoked due to improper use and/or abusive conduct.

   The following practices should be followed when using university e-mail:
   a) No person shall harass others by sending annoying, threatening, libelous, sexually, racially, or religiously offensive messages. This includes all materials deemed offensive by the existing university cold of conduct laws.
   b) Only use Cheyney email for Cheyney related business
   c) Only open emails and/or attachments that you can identify. Do not reply and/or open emails that up here suspect; they may contain viruses' and/or SPAM. Delete all unknown emails and/or attachments.
   d) Never send or forward unsolicited emails or chain mail messages.

II. Prohibit Uses

1. Use of University Information Technology (IT) resources must comply with state and Federal Law, State Systems 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 on the other person's computer, directories, files, or data communications whether protected or not all 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 ID's 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 person shall abide by the terms of the software licensing agreements and copyright laws.
5. Copyright infringement, including illegal file sharing of video, audio, software or data is strictly prohibited.
6. Users of University Information Technology (IT) resources shall not consume unreasonable amount of these resources. The University may impose restrictions or

limits on use of such resources. Deliberate acts which are wasteful or computing/information network resources or which unfailing 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. Printing multiple copies of any document including handouts or announcements is also prohibited.

7. Interfering with security mechanisms or integrity of university technology resources.
8. Performing acts that impede the normal operation of or interfere with the proper functioning of university technology resources.
9. No person shall harass others by sending harassing, annoying, threatening, libelous, sexually, racially, or religiously offensive messages. This includes all materials deemed offensive by existing University code of conduct laws.
10. 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.
11. Excess of or prohibiting use of university technology resources by employees.
12. Unauthorized solicitations on behalf of individuals, groups, or organizations.
13. Intentionally or knowingly installing, executing, or providing to another program or file or any university technology resource that could result in damage to any file, system, or network. This includes, but is not limited to viruses, trojan horses, worms, spyware, or any other malicious programs or files.

III. Disciplinary consequences

The university reserves the right to limit or restrict computing/network privileges to its IT resources. Depending on the seriousness of the defense, 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)].