SECTION:	NO.\			
Security	**2.1.15**			
CHAPTER:	ISSUED:	REV. A	REV. B	REV. C
General	9/11/96	6/26/00	9/27/00	8/18/04
POLICY:	PAGE **1**	OF	**8**	
Fair, Responsible, and Acceptable Use Policy.				

PURPOSE

The purpose of this document is to establish and promote the ethical, legal, and secure use of computing and electronic communications for all members of the Creighton University (referred to in the document as either CU or the University) community. This document complements the CU student handbook and is meant to establish our community policy for FAIR, RESPONSIBLE AND ACCEPTABLE USE OF ELECTRONIC RESOURCES.

Creighton University cherishes freedom of expression, the diversity of values and perspectives inherent in an academic institution, and the value of privacy for all members of the CU community. At the same time, CU may find it necessary to access and disclose information from computer and network users' accounts to the extent required by law, to uphold contractual obligations or other applicable CU policies, or to diagnose and correct technical problems. For these reasons, among others, the ultimate privacy of messages and files cannot be ensured. In addition, system failures may lead to loss of data, so users should not assume that their messages and files are secure.

Although CU does not typically block access to online content, it reserves the right to do so in cases where online content or activity diminishes the capacity of our network or threatens the welfare of Creighton University or its core academic mission. While CU does not position itself as a censor, it reserves the right to limit access to its networks or to remove material stored or posted on campus computers when applicable CU policies, contractual obligations, or state or federal laws are violated. Alleged violations will be treated with the same fundamental fairness as any other alleged violation of CU policy, contractual obligations, or state or federal laws.

SCOPE

This policy applies to all users of computer resources owned or managed by Creighton University, including, but not limited to, CU faculty and visiting faculty, staff, students, external persons or organizations and individuals using CU resources to access network services, such as the Internet and Intranet.

POLICY

Introduction

Creighton University (CU) values technology as a means of communicating information and ideas to the CU community and the world. In keeping with Creighton's commitment to utilize technology in teaching and learning, this policy provides direction in the appropriate use of all forms of electronic resources on campus. This document articulates Creighton University Policy on Fair, Responsible and Acceptable Use of Electronic Resources, provides examples of violations and outlines procedures for reporting, and addressing policy violations.

General Restrictions and Disclaimers

While the use of CU electronic resources may be a requirement for coursework and work, access and use may be restricted or revoked in cases of misuse or repeated abuse. CU reserves the right to limit access to its electronic resources when applicable CU policies, state and/or federal laws or contractual obligations are violated. CU does not, as a rule, monitor the content of materials transported over its network or information posted on CU-owned computers and networks, but reserves the right to do so. Although Creighton University does not typically block access to online content, it reserves the right to do so in cases where online content or activity diminishes the capacity of our network, or where there is a threat to Creighton University or its core academic mission. CU provides reasonable security against intrusion and damage to files stored on the central computing facilities, but does not guarantee that its computer systems are secure. CU may not be held accountable for unauthorized access by other users, nor can Creighton University guarantee protection against media failure, fire, floods, or other natural or man-made disasters.

Use of Resources

All users of Creighton University electronic resources are expected to utilize such resources in a responsible, ethical and legal manner consistent with CU mission and policies. As a user of Creighton University electronic resources, you agree to be subject to the guidelines of this Policy on Fair, Responsible and Acceptable Use of Electronic Resources.

Policies on Fair, Responsible and Acceptable Use

The following policy statements, in ***Bold Italics,*** are accompanied by specific examples that highlight types of activities that constitute unfair, irresponsible or unacceptable use of CU electronic resources. Please note that these examples are provided for the purpose of illustrating each policy's intent and are not intended to be an exhaustive list of all possible scenarios within the policy framework.

Creighton University electronic resources may not be used to damage, impair, disrupt or in any way purposefully, recklessly, or negligently damage Creighton University networks or computers or external networks or computers.

For example, you may not:

1. Use CU electronic resources to breach security of any computer system
2. Knowingly give passwords or ID's for others to use
3. Use computer resources to send large amounts of email (e.g., email "spamming") to an internal or external system
4. Send email of any type to someone's address in an effort to disable their email capabilities

5. Run DNS or DHCP servers that interfere with the Creighton's network
6. Run a personal network or wireless network that interferes with the Creighton's network
7. Forge, alter or willfully falsify electronic mail headers, directory information, or other information generated and/or maintained by Creighton University
8. Use computer resources irresponsibly or in a manner that adversely affects the work of others. This includes intentionally, recklessly or negligently (1) damaging any system by introducing computer "viruses" or "worms," (2) damaging or violating information not belonging to you, or (3) misusing or allowing misuse of computer resources , or (4) tampering with, obstructing, modifying or otherwise damaging or moving/removing electronic equipment.
9. Use Creighton University resources for non-University related activities that unduly increase the network load (e.g., chain mail, network gaming and spamming)

Unauthorized access, reproduction or use of the resources of others is prohibited.

For example, you may not:

1. Access computer accounts or files for which you are not authorized
2. Make unauthorized copies of copyrighted materials. You should assume all software, graphic images, music, and the like are copyrighted. Copying or downloading copyrighted materials without the authorization of the copyright owner is against the law, and may result in civil and/or criminal penalties, including fines and imprisonment.
3. Create or execute any computer programs intended to (a) obscure the true identity of the sender of electronic mail or electronic messages, (b) bypass, subvert, or otherwise render ineffective the security or access control measures on any network or computer system without the permission of the owner, or (c) examine or collect data from the network (e.g., a "network sniffer" program)
4. Use electronic resources to gain unauthorized access to resources of Creighton University or other institutions, organizations or individuals
5. Use false or misleading information for the purpose of obtaining access to unauthorized resources
6. Access, alter, copy, move or remove information, proprietary software or other data files without prior authorization
7. Use electronic resources to discover another individual's password
8. Use electronic resources to obtain personal information (e.g. educational records, grades, or other CU files) about individuals without their permission
9. Use electronic resources to forge an academic document
10. Use electronic resources to take without authorization another person's work or to misrepresent one's own work

11. Use electronic communication to collude on examinations, papers, or any other academic work
12. Use electronic resources to falsify or fabricate research data
13. Use electronic resources to obtain or release another individual's or entity's proprietary information or trade secrets
14. Use Creighton University electronic resources for remote activities that are unauthorized at the remote site
15. Intercept transmitted information intended for another user
16. Scan computers for open or used ports

Use of Creighton University electronic resources to interfere with or cause impairment to the activities of other individuals is prohibited

For example, you may not*:*

1. Send chain email or information about pyramid schemes
2. Send large quantities of email to an individual's mailbox (e.g., email "spamming") which has the effect of interfering with or causing impairment to that individual's activities
3. Change an individual's password in an effort to access his/her account
4. Communicate or use any password, personal identification number, credit card number or other personal or financial information without the permission of its owner

Use of Creighton University electronic resources to harass, create a hostile work environment, make threats to specific individuals, or a class of individuals, is prohibited

For example, you may not:

1. Send unwanted and repeated communication by electronic mail, voicemail or other form of electronic communication
2. Send communication by electronic mail, voicemail or other forms of electronic harassing or inciting communication which are motivated by bias on grounds of race, ethnicity, religion, gender, or sexual orientation (including, without limitation, any communication that violates the University's "Statement Against Discrimination or Harassment")
3. Use email or newsgroups to threaten, stalk or harass someone
4. Create a hostile environment by posting, sending or viewing illicit or inappropriate material
5. Post or send via any form of electronic communication personal or sensitive information about individuals that may harm or defame

6. Post or distribute via any form of electronic communication "hate speech" regarding a group's or individual's race, ethnicity, religion, gender, or sexual orientation

Use of CU electronic resources in pursuit of unauthorized commercial activities is prohibited

For example, you may not:

1. Use computer resources for personal commercial gain, or other commercial purpose without approval by Creighton University
2. Use computer resources to operate or support a non-University related business
3. Use computer resources in a manner inconsistent with Creighton University's contractual obligations to suppliers of those resources or with any published policy of the University
4. Use your University granted web-space for personal monetary gain (this includes clickable ads and pay-per click banners) without approval by the University
5. Register domain names to Creighton University network without proper approval in advance

Use of CU electronic resources to violate city, state, federal or international laws, rules, regulations, rulings or orders, or to otherwise violate any CU rules or policies is prohibited.

For example, you may not:

1. Place software on university-owned equipment that is not legally obtained; such use must follow license and copyright laws as well as DoIT policies.
2. Pirate software, upload or download music (MP3s, videos, etc) and images in violation of copyright and trademark laws
3. Effect or receive unauthorized electronic transfer of funds
4. Disseminate child pornography or other obscene material
5. Create a hostile environment by posting, sending or viewing illicit or inappropriate material
6. Violate any laws or participate in the commission or furtherance of any crime or other unlawful or improper purpose

JayNet Issues

The following are Appropriate Usage Policy items that apply specifically to Creighton University Residence Hall Network (JayNet). These items deal with the disruption of the campus network, in particular, and are therefore not allowed. All JayNet users are expected to abide by all

guidelines mentioned herein when using these resources. It is understood that all items listed above will also apply to appropriate JayNet computing use.

- Only computers that have been registered for JayNet through CUOne may be connected to the network.
- JayNet services, equipment, wiring or jacks may not be altered nor extended beyond the location of their intended use.
- JayNet may not be used to provide access to the Internet by anyone not formally affiliated with Creighton University, except by explicit written consent from University officials.
- Creighton University networks are shared resources. Excessive or improper use of network resources which inhibits or interferes with the use of these networks by others is not permitted.
- Users who connect computers to JayNet that are used as servers, or who permit others to use their computers, whether directly or through user accounts, have the additional responsibility to respond to any use of their server that is in violation of this Appropriate Usage Policy. Server administrators and those who permit the use of their computers by others must take steps to prevent occurrence of such violations and report these violations to the JayNet Support Coordinator.
- In no case shall the following types of servers be connected to JayNet: DNS, DHCP, BOOTP, WINS, or any other server that manages network addresses.
- DoIT shall have the sole authority to assign host names and network addresses to computers attached to JayNet. Thus, a user may not manually configure his/her computer to use a host name or network address that is not assigned to them by DoIT.
- DoIT reserves the right to require immediate, temporary disconnection of any computer that is sending disruptive signals to the network as a whole, whether because of a defective cable, Ethernet card, or other hardware or software problem. It will be the student's responsibility to correct any such problem before the computer can be again connected to JayNet. Noncompliance with this directive will be immediately referred for judicial response.
- DoIT reserves the right to require immediate, temporary disconnection of any computer for the purpose of network hardware, software, or security

troubleshooting, and to enforce the Appropriate Usage Policy. Noncompliance with this directive will be immediately referred for judicial response.

Enforcement of the AUP

DoIT shall have the authority to examine files, passwords, and account information on central servers to protect the security of University computing resources and its users. Violations of this Appropriate Usage Policy will be adjudicated, as appropriate, by Judicial Affairs, Academic Deans' or Vice Presidents' offices. Sanctions as a result of violations of these regulations may result in any or all of the following:

- Loss of University computing privileges;
- Disconnection from JayNet;
- University judicial sanctions as prescribed by the student Code of Conduct;
- Monetary reimbursement to the University or other appropriate sources;
- Separation from the University
- Loss of employment
- Prosecution under applicable civil or criminal laws

DEFINITIONS

Electronic Resources

All computer-related equipment, computer systems, software/ network applications, interconnecting networks, facsimile machines, voicemail and other telecommunications facilities, as well as all information contained therein (collectively, "electronic resources") owned or managed by CU.

ADMINISTRATION AND INTERPRETATIONS

This policy shall be administered by Information Security. Questions regarding this policy should be directed to the Information Security Officer.

AMENDMENT/TERMINATION OF THIS POLICY

The University reserves the right to modify, amend or terminate this policy at any time. This policy does not constitute a contract between the University and its faculty or employees.

REFERENCES TO APPLICABLE STANDARDS

None

EXCEPTIONS

None

VIOLATIONS/ENFORCEMENT

Any known violations of this policy should be reported to the University's Information Security Officer at 402-280-2386 or via e-mail to infosec@creighton.edu.

Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with University procedures. The University may advise law enforcement agencies when a criminal offense may have been committed.