SERIES NUMBER: 843

TITLE: **Personnel**

Information Systems Policy

Dodge City Community College (DCCC) provides computing resources and worldwide network access to its faculty, staff and currently enrolled students for legitimate administrative, educational and research efforts. Access to the DCCC computing resources is a privilege and DCCC reserves the right to restrict, limit or extend computing privileges and access to its information systems. As a member of the DCCC electronic community, it is the responsibility of each individual to use computing resources in a responsible, ethical and legal manner.

The DCCC Management and Information Systems (MIS) will make every effort to ensure that access is available at all times; however, the user must understand the system may not always be available for use due to maintenance, testing, backups, power failures, or other circumstances beyond our control. Access at any given time is not guaranteed.

No Expectation of Privacy

Access to DCCC computing resources is a privilege. DCCC retains custody, control and supervision of all computers, networks and internet services owned or leased by DCCC. DCCC reserves the right to intercept, monitor, copy, review and download all computer and internet activity by anyone with access to the system. No one accessing DCCC computers, networks and internet services has an expectation of privacy in their use, including e-mail messages and stored files. Anyone with access to the DCCC computing resources is expected to use appropriate judgment and caution in communications concerning students and staff to ensure that personally identifiable information remains confidential.

Responsibilities

Anyone with access to DCCC computing resources shall:

- Protect user ID and passwords from unauthorized use. MIS should be contacted immediately if there is reason to believe someone has unauthorized access to a user ID and/or password(s).

- Not share user ID or passwords. The use of faculty/staff computers is for employees only and each individual is responsible for all activities on the assigned ID.

- Access only files and data the user has been given authorization to access or is available to the public.

- Use only approved legal versions of copyrighted software in compliance with vendor license requirements.

- Be considerate in use of shared resources by not monopolizing systems, overloading networks with excessive data (spamming), or wasting computer time, connect time, disk space, printer paper and toner and other computing resources.

- Be aware that e-mail may be considered public record and subject to public access pursuant to the Kansas Open Records Act.

- Install and maintain current virus protection software on your computer.

<u>Unacceptable Uses</u>

Unacceptable use of computing resources includes the following**:**

- Disclosure of passwords or use of another individual's user ID, password~~s~~, or security privileges to gain access to networks or computing systems for which they do not have security. This includes allowing students access to a computer assigned to faculty or staff.

- Masking identity of an account or machine. This includes mail that appears to come from someone other than the individual sending the mail.

- Use of e-mail or message services to harass, intimidate, threaten, or otherwise annoy another person by use of sexual**,** ethnic or racial content or content which poses an imminent threat to the life or safety of the person(s) receiving the communication.

- Storing, distributing, editing or recording sexually explicit e-mails or materials, except when directly related to an approved course or other DCCC educational activity.

- Use of another individual's files or data without express permission from that person.

- Use of computer programs to decode passwords or access controlled information.

- Engaging in any activity that may be harmful to the systems or to any information stored on the systems, such as creating or propagating viruses, worms, Trojan horses, disrupting services, spamming or damaging files.

- Running or configuring software or hardware to intentionally allow unauthorized access or to bypass system security.

- Attaching personal computer equipment to a DCCC computer or network. (Laptops, PDA's, etc.)

- Intentionally damaging or destroying files, equipment, software or data belonging to DCCC or others.

- Making, using, storing or distributing copies of copyrighted software or other copyrighted materials (such as digitized artistic productions) without proper legal authority**.**

- Using DCCC systems for commercial use, personal gain, or other unauthorized activity. For example, performing work for profit or advertising in a manner not authorized by DCCC or distributing unsolicited advertising, sending/forwarding chain letters, solicitations or other unauthorized use.

- Installing or operating computer games on DCCC owned or leased equipment for purposes other than academic instruction.

- Posting web pages that contain profane, intimidating, or illegal material or promote illegal activity (i.e. gambling, obscenity, or sexual harassment).

- Violation of any DCCC or Kansas Board of Regents policy or any local, state or federal law.

- Unnecessary mailings to an entire group, such as all DCCC users. Group mailings should only be made when absolutely necessary, and should be limited to items directly related to the business activity and/or mission of DCCC.

- Using the DCCC networks or computing systems for personal use or any business or activity not related to DCCC business or activities.

Persons using DCCC provided computing resources shall be familiar with DCCC policies and rules. Misinterpretation or misunderstanding of DCCC policies and rules shall not be a mitigation of responsibility. Questions regarding acceptable use of any computing resources should be directed to the Information Technology Director at 227-9253.

Reporting Violations

Department heads have authority to deny access to any DCCC system(s) under their supervision. Awareness of any security problem affecting any DCCC computer or network facility shall be communicated to the Information Technology Director at 227-9253.

Consequences of Misuse

Misuse of DCCC computing resources is unacceptable and users will be held accountable for their conduct. Failure to comply with this policy or any other established procedures or rules governing the use of computing resources and network access will be subject to disciplinary action, up to and including termination of employment. Further, illegal use of DCCC computing resources or network access may be referred to law enforcement authorities.

Employees who violate this policy shall be responsible for any resulting loss, costs or damages incurred by DCCC. Any questions regarding this policy should be directed to the Information Technology Director at 620-227-9253, Office of the Dean of Instruction at 620-227-9359 or the Dean of Student Services at 620-227-9203.

DATE OF ADOPTION:	November 20, 2003	**LEGAL REFERENCE: K.S.A.**
REVIEW DATE(S):	February 28, 2007	**N/A**

DODGE CITY COMMUNITY COLLEGE
INFORMATION SYSTEMS POLICY

RECEIPT AND ACKNOWLEDGMENT

DO NOT SIGN YOUR NAME ON THIS RECEIPT AND ACKNOWLEDGMENT UNTIL AND UNLESS YOU HAVE CAREFULLY AND COMPLETELY READ BOARD POLICY NO. 843 AND ASKED ANY QUESTIONS YOU MAY HAVE CONCERNING IT.

I acknowledge I have read and understand the contents of the Information Systems Policy attached hereto. I agree to abide by the terms of the policy and understand that failure to comply with the terms of the policy may result in disciplinary action, up to and including termination of employment.

I further understand that illegal use of Dodge City Community College computing resources may result in referral to law enforcement authorities and/or legal action.

Failure to consent to comply with the Dodge City Community College Information Systems Policy or refusal to acknowledge receipt of a copy of Board Policy No. 843, in writing, shall result in the immediate removal of all privileges to access and/or otherwise use the Dodge City Community College information systems.

____
Employee
Printed Name: ______________________

Date: ____________________________

____
Witness