

Caldwell Community College and Technical Institute
Student Computer Usage Policies and Procedures

I. PURPOSE:

The purpose of this section is to define the policies and procedures for the usage of the administrative systems, computer resources and network systems at Caldwell Community College and Technical Institute.

II. PROCEDURE:

A. INTRODUCTION

Caldwell Community College and Technical Institutes utilize microcomputer systems that are accessed by employees and students to facilitate the performance of their duties. These duties include, but are not limited to, data entry and retrieval, report preparation, records maintenance, instruction, research, and planning. Because of this wide range of users and uses, it is necessary to establish policies and procedures that insure that the systems are used in the most efficient way possible while providing for the protection of equipment, data, and software. While the Director of Computer Information Services is charged with responsibility for the proper use of the computer systems, it is every employee and every student's responsibility to see that the computers are properly used and that security is maintained.

B. POLICY

Students of the College are directly responsible for the integrity of each microcomputer system for the period of time they use the system. Student microcomputer system users must be aware of and employ proper operating procedures to assure security. Access to the systems will be on a "need to know" basis considering the accomplishment of assigned duties. In this context, "the system" means both the equipment and the data. Requests for access will be approved first by the appropriate instructor or dean before being routed to the Director of Computer Information Services for approval.

C. PROCEDURES

1. SECURITY

Security refers to the protection of all equipment resources from any kind of damage and the protection of data from (1) disclosure to any unauthorized person, (2) unauthorized modification, or (3) destruction. While disclosure or damage may occur accidentally or intentionally, the results are the same. The security system implemented in these procedures will, if used properly, prevent the previously mentioned occurrences from happening.

- a. Basic access to the College computer system is controlled through User ID and password protection. Each computer system has a personal ID that must not be used by any other user. The College Executive Council reserves the right to authorize the Computer Information Services Staff to override user accounts and computer systems if sufficient evidence of inappropriate usage exists.
- b. Student users should not leave their microcomputer systems unattended. If a user must leave the immediate area of his/her workstation for an extended period of time, he/she should log off the system. Sensitive information should not be left unattended or sent to printers that are located in areas open to the public.

- c. Students are responsible for reporting suspected security violations to the Computer Information Services staff immediately. The Computer Information Services staff will investigate the violation and take appropriate action where required.
- d. Physical access to the centralized system is strictly controlled by the Computer Information Services Staff. Students will not be allowed to enter the computer room unless authorized by a member of the Computer Information Services Staff. There will be no exceptions to this policy.

2. MICROCOMPUTER AND NETWORK SYSTEMS

In addition to the administrative and student computing systems, the college owns a large number of other computing devices -- primarily microcomputers. Although the security problems with stored data are smaller when dealing with microcomputers, issues concerning the use and protection of software are of major concern. The college does not purchase microcomputer software outright, but purchases a "software license" which allows the college to use the software but severely restricts anything other than the use of the software on a single computer or network. With this in mind, the following must be adhered to:

- a. **SOFTWARE:** Unless specifically authorized in writing by the software developer or publisher, programs and their related documentation shall not be reproduced in any form. U. S. Copyright Law provides for civil damages of \$50,000 or more and criminal penalties, including fines and imprisonment, in cases involving the illegal reproduction of software. Students cannot install software on College-owned microcomputers unless authorized by an employee of the College. Students involved in the making or use of unauthorized copies of computer software will be subject to disciplinary action as appropriate under the circumstances. Unauthorized copies or illegal software installed by students will be confiscated and destroyed. Software licensed to the college will not be removed from the campus without the specific written permission of the Director of Computer Information Services.
- b. **ELECTRONIC MEDIA:** Computer Information Services will practice appropriate measures to provide security, operability and integrity to the Wide Area Network, hereafter referred to as WAN, including e-mail, Internet, and other related resources. The College will not guarantee that electronic media stored on microcomputers and transmitted on the WAN will remain confidential and secure. Additionally, computer related files and data created or stored on College microcomputer systems are considered open records and are subject to discovery and subpoena during disciplinary and legal actions. The College reserves the right to view, monitor, and disclose the contents of e-mail and data created, transmitted, received, and stored on College owned microcomputers in the following circumstances:
 1. Investigations that reveal evidence of misconduct and misuse of accounts.
 2. Need to protect the general welfare of the college employees and students.
 3. Need to prevent interferences with the mission of the college.
 4. Illegal activity that violates federal, state, or local regulations.
- c. **AUTHORIZED USAGE:** Microcomputer users should not deliberately attempt to modify or degrade the performance of college owned systems. The systems are provided as a service and should be used to complete College-related assignments and research, not for personal business or recreation. The college computer systems must not be used to intercept data, monitor user accounts, gain unauthorized access, restricted data, or for any purpose that violates federal, state or local regulations.

- d. **MORALS AND ETHICS:** Freedom of expression is a constitutional right afforded to individuals. However, Microcomputer System Users are held accountable for their actions and will respect the rights of individuals who may be offended by the services and images retrieved on the Internet. Individuals who feel they have been harassed should report the incident to the Director of Computer Information Services.

- e. **VIOLATIONS:** A student who learns of a violation of these policies shall report it to a member of the College faculty or Computer Information Services Staff as soon as possible. Violators of the computer usage policies and procedures previously stated will be subject to one or more of the following sanctions: admonition, temporary or permanent suspension of computer access privileges, or dismissal from the College as stated in the Student Handbook.

Adopted by the Board of Trustees on June 15, 2000