ADMINISTRATIVE RULE

Approval Date: 12/10/12
Effective Date: 12/10/12
Last Revised: 03/11/20

Rule Number/Name:	080.001.000 – Electronic Communication System
Responsible Department:	Information Technology Services
Authority:	Executive Director of Infrastructure

Overview

The College's Electronic Communications Systems (ECS) and Electronic Information Resources (EIR) include all electronic devices, infrastructure, and processes used to transmit or receive information.

All college information, records and files, including those stored electronically, are property of Columbia Gorge Community College. Regulations and responsibility for safeguarding, recording or accessing these records are governed by policies, procedures, rules and statutes of Columbia Gorge Community College, State of Oregon and the United States Government.

The College's Electronic Communications Systems (ECS) are provided for (1) students to engage in educational and research activities related to College classes and (2) employees and faculty to conduct business and engage in other activities related to the performance of their job functions.

Applicability

Staff, Faculty, Students, and Community Members

Exception to policy: The CGCC Library is open to the public and computers located in the Library at The Dalles Campus and in the Information Commons at the Hood River-Indian Creek Campus are available for use by the public, with priority access given to students doing academic research or class work.

Any changes made to the ECS will be provided to employees via their college provided email account within 30 days of changes being adopted.

Nothing in this administrative rule is designed to conflict with any provision in any collective bargaining agreement.

Administrative Rule Statement

Access to the College's ECS is authorized to the following:

- College employees;
- Faculty;
- Students; and
- Others as authorized by the College president.

By law (including but not limited to FERPA, HIPAA and Social Security regulations), most data is confidential and cannot be released by the College without proper authorization. Each employee is responsible for understanding the confidentiality requirements of the data to which he/she has access.

Users are permitted to use the College's ECS only in furtherance of the function that results in authorized access: for students to engage in educational and research activities related to College classes; for employees and faculty to conduct business and engage in other activities related to the performance of their job functions.

The College has the ability to remotely monitor or control any computer on the College network. User authorization to remotely access a computer and a visual note signifying remote access is being performed on the remote accessed computer, will be implemented whenever possible.

Supervisors have the right to gain access to their staff's network and local computer data.

General Guidelines and Prohibitions

Operation of the College's ECS relies upon the proper conduct and appropriate use by all users. Students, faculty, staff, and others granted system access are responsible for adhering to the following prohibitions and guidelines.

A. General Guidelines

ECS users will:

1. Adhere to the same standards for communicating on-line that are expected for other types of communication throughout the College and are consistent with Board policy and administrative procedures.

2. Not knowingly and consistently make use of computer resources in any manner that interferes with the ability of others to make equal use of those same resources. (Examples: Network use, broadcast of unsolicited email and messages, network disk utilization, and Internet bandwidth usage)

3. Schedule communications intensive activities such as large file transfers, mass e-mailings, and streaming audio or video for off-peak times (before 8 am or after 5 pm Monday through Friday).

4. Be aware of your network storage utilization and remove files that were for temporary use, or are no longer needed.

5. Respect the privacy of others.

6. Cite all documents and information accessed via Internet that are used in reports, term papers, journal articles, etc. with a proper bibliographic reference. Not including proper citation for sources of information is plagiarism and will be treated as such.

7. Internal mass emails must be in regard to College business, on Campus Event, College sponsored event, or College related event. Users sending an email to staff@cgcc.edu or faculty@cgcc.edu must place those addresses in the BCC field.

8. Protect password confidentiality. Passwords are not to be shared with anyone, including ITS staff. ITS staff are not able to view passwords.

9. Be forgiving of the mistakes of others and share your knowledge. Practice good mentoring techniques.

10. Be individually responsible for not pirating copyrighted or licensed software and related materials, such as documentation, etc.

11. Use of the ECS or Internet should not invade the privacy of others. Federal laws protect the privacy of users of wire and electronic communications. All data should be treated as confidential unless designated or authorized for public use. This authorization is usually signaled by the user setting file access permission to allow public or group reading of the files. If in doubt, ask the Chief Technology & Planning Officer.

12. Promptly report security problems or misuse of the system to the Executive Director of Infrastructure; Information Systems Security Manager; or for Library resources, report to the library staff.

13. Follow the established Computer Usage Procedures.

14. Modify College network password as follows:

    1. Valid for 365 days
    2. Must be at least 8 characters in length
    3. Not reused from previously used passwords
    4. Follow any three of the following four rules:
        1. Use at least one uppercase letter
        2. Use at least one lowercase letter
        3. Use at least one number
        4. Use at least one special character

B. Prohibitions

1. It is a violation of this Administrative Rule to engage in or attempt to engage in the following conduct:
    1. Using the system for commercial or personal gain purposes, e.g., consulting for pay, sales of any kind, etc.
    2. Using the system to avoid personal expense.
    3. Using, reproducing or distributing material on the system in violation of copyright law or applicable provisions of use or license agreements.
    4. Degrading, disrupting or vandalizing the College's equipment, software, materials, or data or those of any other user of the system or other networks connected to the system. This prohibition includes attempts to gain unauthorized access to restricted information or networks; make unauthorized entry to files, accounts or networks inside or outside the

College; or intentionally seek information on, obtain copies of, or modify files, other data or passwords belonging to others without their explicit permission.

5. Subscribing another person to a bulletin board or discussion group, plant or distribute viruses, or use or distribute unauthorized software or other resources.

6. Evading, changing, or exceeding resource quotas or disk usage quotas.

7. Intentionally accessing, downloading, or transmitting any text file or picture or engage in any conference that includes material which constitutes harassment of others; or encourages commission of unlawful acts or violation of lawful Board policies and/or administrative procedures.

8. Accessing any service via the College's system that has a cost involved or attempts to incur other types of unauthorized costs. The user accessing such services will be responsible for these costs.

9. Posting or publishing personal information, including photographs, age, home, or work addresses or phone numbers or other personal data of another person.

10. Using the system, EIRs or Internet to store personal information about individuals that they would not normally freely share with others about themselves. Collect information about individual users without their consent.

11. Intercepting or otherwise monitoring any Internet or any system communications not explicitly meant for you.

12. Using the ECS, EIRs, or Internet in violation of federal, state and local laws.

13. Loading or installing any programs, personal files, personal data or software on any computer or the network, unless authorized by the Executive Director of Infrastructure.

14. Using the ECS for non-College-related downloading, uploading, or sharing music, video streaming, playing games, or other high-bandwidth activities

2. Unauthorized attempts to upload information to or change information on this service are strictly prohibited and may be punishable under the state law and federal statutes including the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act of 1996.

3. Material that is fraudulent, abusive, discriminatory, sexually explicit, profane, obscene, defamatory, or otherwise unlawful or inappropriate may not be intentionally sent by e-mail or other form of electronic communication (such as bulletin board systems, newsgroups, or chat groups) *or displayed on or stored in* CGCC's computers. Users encountering or receiving this kind of material should immediately report the incident to their supervisors.

4. The College's Sexual Harassment and Non-Discrimination Policies and Procedures apply also to Internet, EIRs and the ECS. Sending or forwarding offensive, intimidating or insulting mail or messages may constitute harassment and is a violation of the intended educational and administrative use of Internet, EIRs and the network, and may result in loss of Internet, EIRs and/or system privileges, and/or be reported to law enforcement.

5. The College reserves the right to delete, move or edit messages that it, in its sole discretion, deems in violation of copyright or trademark laws, or otherwise unacceptable. Users shall remain solely responsible for the content of their messages.

6. Chain letters waste computing resources and may be considered harassment. Creating or forwarding chain letters will result in loss of Internet, EIRs and system privileges.

7. Connecting ECS equipment to the College's system without written authorization.

    1. Examples but not limited to: network devices such as printers, IP phones, switches/hubs/routers/wireless networking devices, non-CGCC desktops or laptops, etc.

8. Modifying ECS equipment without written ITS authorization.

9. Installing software on any College ECS equipment without written ITS authorization. Performing updates to existing software is allowed.

C. Violations/Consequences

1. Students

1. Violations of this Administrative Rule will be dealt with in the same manner as violations of other college Board Policies, Administrative Rules, or established procedures, and may result in disciplinary review. In such a review, the full range of disciplinary sanctions is available including the loss of computer use privileges, dismissal from the college, and legal action. Violations of some of the above prohibitions may constitute a criminal offense.
2. Violations of law will be reported to law enforcement officials.

2. Faculty and Staff

1. Faculty and staff who violate this Administrative Rule will be subject to discipline, up to and including dismissal in accordance with negotiated agreements and applicable provisions of law.
2. Violations of law will be reported to law enforcement officials.

3. Others

1. Other users who violate this Administrative Rule shall be subject to suspension of College ECS access, up to and including permanent loss of privileges.
2. Violations of law will be reported to law enforcement officials.

Information Content/Third Party Supplied Information

Opinions, advice, services, and all other information expressed by ECS users, information providers, service providers, or other third parties are those of the providers and not the College.

The College does not warrant that the function or services performed by the ECS or that the information or software contained on the ECS will meet the ECS user's personal requirements. In addition, the College does not warrant that the ECS will be uninterrupted or error-free or that defects can be corrected. The College's ECS is provided on an "as is, as available" basis. The College does not make any warranties, whether express or implied including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the ECS and any information or software contained therein.

CGCC is not responsible for material viewed or downloaded by users from the Internet. The Internet is a worldwide network of computers that contains millions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material. In general, it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. In addition, having an email address on the Internet may lead to receipt of unsolicited e-mail containing offensive content. Users accessing the Internet do so at their own risk.

Columbia Gorge Community College reserves the right to modify this Administrative Rule at any time. Questions about this Administrative Rule should be addressed to the Executive Director of Infrastructure, or the President.

Definitions

None

Interpretation of Administrative Rule

Chief Technology and Planning Officer

Cross Reference to Related Administrative Rules

1. CGCC Administrative Rule 010.001.000 - Copyright and Fair Use
2. CGCC Administrative Rule 010.002.000 - Copyright Guidelines for Specific Media

Further Information

Executive Director of Infrastructure
ddehaze@cgcc.edu
(541) 506-6090

Strategic Direction

- KFA 2: Students
- KFA 3: Faculty and Staff
- KFA 8: Technology

Appendix

1. Information Technology Electronic Communications System Policy Acknowledgment
2. Computer Fraud and Abuse Act, http://energy.gov/sites/prod/files/cioprod/documents/ComputerFraud-AbuseAct.pdf