Columbia Gorge
Community College

Electronic Communications System (ECS):
Electronic Information Resources (EIR) and Internet Policy

Basic Policy

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

The users of the College’s ECS should treat one another with respect and professionalism. Such conduct includes: consideration of others, responsibility for one’s actions, respect for College property and authorized and efficient use of College resources. Users of the ECS, EIRs and Internet should have a basic understanding of the law regarding copyright and other legal issues.

The College does not guarantee that messages or files are private or secure. The College administration has access to all messages and files on the ECS. The College reserves the right to monitor all use of the College’s ECS, electronic resources, and Internet access randomly or to assess compliance with these procedures. All users are required to cooperate with College efforts to monitor system usage and to investigate possible violations of these procedures. Upon request of the College, a user must promptly demonstrate the appropriate basis for use of the system.

Electronic Communications System (ECS) Access

A. Access to the College’s ECS is authorized to the following:
   1. College employees.
   2. Faculty.
   4. Others as authorized by the College president.

B. 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.

C. The College will monitor ECS usage. Users understand that CGCC may use automated software to monitor material created, stored, sent or received on its ECS. Upon request of the College, a user must promptly demonstrate the appropriate basis for use of the system. Users should not have an expectation of privacy in anything they create, store, send or receive on the ECS.
D. The College has the ability to remotely monitor or control any computer on the College network. User authorization to remotely access a computer and visual verification on the remote computer will be implemented whenever possible.

E. 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 throughout the College and are consistent with Board policy and administrative procedures.
2. Should 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 8am or after 5pm Monday through Friday).
4. Be aware of your network storage utilization. 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. Adhere to guidelines for managing and composing effective e-mail messages:
   a. One subject per message, avoid covering various issues in a single message.
   b. Use a descriptive heading.
   c. Do not use all upper case letters, which is considered SHOUTING on Internet.
   d. Be concise, keep message short and to the point.
   e. Cite appropriate references.
   f. Conclude message with actions required and target dates.
   g. Delete unneeded e-mail.
   h. Mass email should follow the “Guidelines for Mass Email”. In summary “The message must be in regard to College business, on Campus Events, or off Campus College related Events, and material in the email must conform to the College’s Acceptable Use Policy.”
8. Protect password confidentiality. Passwords are not to be shared with others.
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, EIRs 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 Information Technologies Director.

12. Promptly report security problems or misuse of the system to the Information Technologies Director; or for Library resources, report to the library staff.

13. Follow the established Computer Usage Procedures.

B. Prohibitions/Procedures

It is a violation of these procedures to engage in or attempt to engage in the following conduct:

1. Use the system for commercial or personal gain purposes, e.g., consulting for pay, sales of any kind, etc.

2. Use the system to avoid personal expense.

3. Use, reproduce or distribute material on the system in violation of copyright law or applicable provisions of use or license agreements.

4. Degrade, disrupt or vandalize 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. Unauthorized attempts to upload information 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.

6. 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.

7. 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.

8. 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.

9. Subscribe another person to a bulletin board or discussion group, plant or distribute viruses, or use or distribute unauthorized software or other resources.
10. Evade, change, or exceed resource quotas or disk usage quotas.
11. Intentionally access, download, or transmit 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.
12. 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.
13. Access 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.
14. Post or publish personal information, including photograph, age, home, or work addresses or phone numbers or other personal data of another person.
15. Use 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.
16. Intercept or otherwise monitor any Internet or any system communications not explicitly meant for you.
17. Use the ECS, EIRs, or Internet in violation of federal, state and local laws.
18. Load or install any programs, files, data or software on any computer or the network, unless authorized by the I.T. Director.
19. Using the ECS for non-College-related downloading, uploading, or sharing music, video streaming, playing games, or other high-bandwidth activities.
20. Attach any equipment to the College’s network, unless authorized by the I.T. Director.

C. Violations/Consequences

1. Students
   a. Violations of these prohibitions will be dealt with in the same manner as violations of other college prohibitions 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.
   b. Violations of law will be reported to law enforcement officials.

2. Faculty and Staff
   a. Faculty and staff who violate the ECS, electronic resources, or Internet prohibitions shall be subject to discipline, up to and including dismissal in accordance with negotiated agreements and applicable provisions of law.
   b. Violations of law will be reported to law enforcement officials.

3. Others
a. Other users who violate the ECS, electronic resources, or Internet prohibitions shall be subject to suspension of College ECS access, up to and including permanent loss of privileges.
b. Violations of law will be reported to law enforcement officials.

**Information Content/Third Party Supplied Information**

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

B. The College does not warrant that the function or services performed by or that the information or software contained on the ECS will meet the ECS user’s requirements or 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.

C. 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 request may lead to sites with highly offensive content. In addition, having an e-mail 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 procedure at any time. Questions about this Procedure should be addressed to the Information Technologies Director, the Executive Director for Resource Development, or the President.