

Policies and Procedures



Internal Policies

[Alphabetic Index](#)
[Board of Trustees](#)
[Budget and Planning](#)
[College Advancement](#)
[Disappearing Task Force \(DTF\) Reports](#)
[Employment Policies](#)
[Faculty Handbook](#)
[Finance and Administration](#)
[Governance and Grievance Procedures](#)
[Health and Safety](#)
[Planning Documents](#)
[Student Affairs](#)
[Washington Administrative Codes \(WAC's\) affecting Evergreen](#)

External Policies, Statutes and Rules

[Resources](#)
[Revised Code of Washington \(RCW\)](#)
[Washington Administrative Code \(WAC\)](#)

Computing and Communications

Appropriate Use of Information Technology Resources

[Purpose](#)

[Scope](#)

[Access/Eligibility](#)

[Roles and Responsibilities](#)

[Privacy and Public Records](#)

[What can be attached to the network and how](#)

[Prohibitions](#)

[Consequences](#)

[Policies and Laws Applicable to Information Technology Systems](#)

Purpose

Evergreen's information technology (IT) systems are a continually growing and changing resource that supports thousands of users. These resources are vital to the work of the entire Evergreen community, and to the full breadth of activities that contribute to the fulfillment of the college's mission.

This appropriate use policy balances campus community needs for flexibility and exploration with Evergreen's need for secure and reliable IT systems. In order to ensure a reasonable and dependable level of service, it is essential that each member of the campus community exercise responsible, ethical behavior when using these resources. Misuse by even a few individuals has the potential to disrupt the legitimate academic work of faculty and students, or the business of the college.

This policy is intended to supplement, not replace, existing laws, regulations, policies

and contracts that currently apply to these resources (see Illustrative Laws and Policies section).

[Top](#)

Scope

This policy applies to all IT system users (see Access/Eligibility below). It covers:

- any and all college owned or managed computer systems (including but not limited to email, web pages, administrative applications, academic applications, personal computers, mini- and mainframe computers, file storage, and all forms of software);
- computer-related equipment (including but not limited to personal digital assistants, wireless devices, facsimile machines, scanners, printers, telephones, video and other multimedia devices, and associated peripherals);
- interconnecting networks;
- any information stored on any of these systems;
- any personally owned equipment on campus that is connected to the college network or equipment connected through Evergreen's modem pools.

[Top](#)

Access/Eligibility

- Information technology resources are provided by Evergreen for use by its Students, Faculty, Staff, and Guests. In addition, Evergreen's library provides access to its resources for the general public.

[Top](#)

Roles and Responsibilities

Users of Evergreen information technology resources have a responsibility to protect these resources, and to respect the rights of others. They are responsible for familiarizing themselves with state and

Contact the Site Manager

Last Updated: November 23, 2007

The Evergreen State College
2700 Evergreen Parkway NW
Olympia, Washington 98505
(360) 867-6000
All content and images on this site
are copyrighted by The Evergreen
State College. © 2007
[Suggest a Link](#)

federal laws that pertain to information technology, as well as the contents of this, and related, college policies (see Illustrative Laws and Policies section). Users of college information technology resources should:

- use resources within the boundaries of college policies and federal, state, and local laws, and rules by adhering to ethical restrictions on use of college property and data ;
- use resources in a manner that does not diminish the reliability or availability of those systems or resources for other users;
- protect their passwords, and prevent unauthorized access to or from their computers and system accounts;
- demonstrate a respect for other user's intellectual property, rights to privacy, or rights to freedom from intimidation, discrimination, and harassment;
- protect college data, and ensure that confidential information isn't stored or displayed in unsafe places;
- comply with security restrictions on all systems.

Unauthorized use of information technology resources is prohibited. Each individual bears the primary responsibility for the material s/he chooses to access, store, send or display. In the case of an activity which isn't specifically cited as either allowed or prohibited in any college policy or state or federal law, users should err on the side of caution: if a use bears a cost to the state, interferes with use of systems by others, or violates the rights of another person, it shall be considered unauthorized.

The college has a responsibility to:

- practice good stewardship of state resources;
- treat information about, and information stored by, the system's users in a manner that respects both user privacy and the value of the information;
- take precautions to protect college information systems and the

- information contained therein from malicious or unauthorized use;
- faithfully execute all hardware and software licensing agreements applicable to college systems;
 - take precautions against theft or damage to system components; and
 - respond to lawful requests for disclosure of information.

[Top](#)

Privacy and Public Records

Evergreen respects the principles of academic freedom, freedom of speech, and the right of privacy. The use of information technology systems holds special implications for these principles.

Information system accounts may provide access to sensitive, restricted or confidential data. Users of college information systems will maintain the confidentiality of any and all data retrieved from TESC information systems. Disclosure of the information to unauthorized persons could subject the user to criminal and civil penalties imposed by the law or disciplinary action imposed by the college.

Data must be stored within a "secure storage device" as designated by Computing and Communications if the unauthorized discloser of the data would subject the organization to a negative operational impact; constitute a violation of federal or state law; or result in harm to the individual or carry significant financial liability. Portable data storage devices (e.g., tape drives, zip drives, removable hard drives, USB data storage devices, etc.) are not designated as secure. Questions regarding secure storage of data should be directed to the Computing and Communications Helpdesk.

The Family Education Rights and Privacy Act of 1974 govern disclosure of records, documents or other facts containing personally identifiable information about students. Requests for information about students, or requests for lists of individual students, are to be forwarded to the college official responsible for maintaining

the information, and questions concerning the release of information should be referred to the Associate Vice President of Enrollment Services or the Registrar.

Other record and documents regarding employees, research data, preliminary drafts, notes and recommendations, as well as requests for lists of individuals which may be used for commercial purposes, may be exempt from, or not subject to, public disclosure. College rules contain additional types of records exempt from disclosure. Disclosure of public records shall be in accordance with Evergreen's policy in WAC 174-276. Requests for non-student records will be forwarded to Evergreen's Internal Auditor.

IT staff shall not routinely inspect nor monitor use of computers. Nor shall they routinely change nor delete files or email from accounts on college-managed systems unless they are invited to do so by the owner of the account. However, ***there can be no guarantee of security and privacy of your email and electronic files***, and the college specifically reserves the right to review, audit, and inspect email and electronic files as state law requires.

In general, an account will only be inspected by the college when:

- activity from an account or network address impedes access to computing or networking resources by others;
- an employee has failed to, or is unable to, respond to a lawful public records request;
- general usage patterns indicate that an account or computer is being used in an inappropriate activity;
- there are credible reports of violations of policy or law taking place;
- it appears necessary to do so to protect the college from liability;
- it is required by and consistent with law (e.g. Evergreen's Patriot Act Policy).

All new employees of the college are to

participate in Security Awareness Training as a part of mandatory orientation training. Continuing employees will annually participate in Security Awareness Training made available by Evergreen.

[Top](#)

What Can Be Attached to the Network and How

In order to maintain the security and reliability of Evergreen's campus network, users are required to abide by the following rules when connecting devices to Evergreen campus networks:

- all computers must have current anti-virus software installed prior to connecting to the campus network;
- users shall not establish network or dial up connections that bypass Evergreen's firewall;
- connection of and/or use of Virtual Private Networks (VPNs) devices or software must be approved in advance by Network Services;
- installation of Wireless Access Points or ad-hoc wireless networks must be approved in advance by Network Services (Wireless Access Points in Housing must be approved by the Housing Technology Manager) .

[Top](#)

Prohibitions

In light of all the policies outlined above in this document, the following are examples of specifically prohibited activities:

- sharing of account/usernames or passwords;
- attempting to test security flaws without Network Service authorization;
- probing or connecting to any computers without legitimate reason to do so;
- using Evergreen systems or networks as a staging ground to crack other systems or networks;
- installing invasive software, such as worms or viruses on any Evergreen

- system over any network;
- altering any data, software, or directories other than your own without proper authorization;
- attempting to gain access to a system, account or password that you are not previously authorized to access;
- using system resources for:
 - unethical purposes, including private outside business or political purposes unless authorized under the Ethics in Public Service Act or rules of the Executive Ethics Board;
 - committing acts of academic dishonesty (see Student Code of Conduct);
 - installing software on state-owned equipment which is not directly tied to the academic or administrative work of the college;
 - installing personal software, games, music, screensavers or other electronic materials which may interfere with the stability or reliability of college owned systems;
 - violating copyright laws (including software, images, music, movies, or text);
 - sexual harassment or harassment based on race, color, gender, religion, creed, age, marital status, national origin, sexual orientation, disability, or veteran status.

[Top](#)

Consequences

Violations of this policy will be investigated by the college and may result in revocation of access to information technology resources and/or disciplinary or legal action. Violators are subject to any and all of the following:

- loss of information technology resources access;
- college disciplinary action (as prescribed in the Student Conduct Code, Union Contract, Faculty Handbook, Human Resource Policies/Procedures, or at the discretion of immediate supervisor

- for exempt staff);
- civil proceedings;
- criminal proceedings.

[Top](#)

Policies and Laws Applicable to Information Technology Systems

UNITED STATES CODE

- [The USA Patriot Act of 2001 and 2003 amendment](#)
- [The Digital Millennium Copyright Act of 1998](#)
- [The U.S. Copyright Act](#)
- [Computer Fraud and Abuse Act of 1986](#)
- [Electronic Communications Privacy Act of 1986](#)
- [Unlawful access to stored communications](#)
- [The Privacy Protection Act of 1980 - 42 USC Sec. 2000aa](#)
- [Public Telecommunications Act of 1992 Telegraphs, Telephones, and Radiotelegraphs 47 USC Sec. 605](#)
- [Interstate Transportation of Stolen Property Act](#)
- [Family Educational Rights and Privacy Act of 1974 \(FERPA\)](#)

REVISED CODE OF WASHINGTON (RCW)

- [Computer Trespass RCW 9A.52.110](#)
- [Malicious mischief- RCW 9A.48.100](#)
- [State resources cannot be used for personal gain - RCW 42.52.160](#)
- [State resources cannot be used for political campaigns - RCW 42.52.180](#)
- [State Ethics Board has the authority to investigate allegations - RCW 42.52.360](#)
- [State computers may not be accessed without authorization RCW 9a.52.110](#)
- [Theft of Telecommunication services- RCW 9A.56.262](#)
- [Disclosure -- Campaign finances -- Lobbying - Records RCW 42.17.260](#)
- [Retention of public records RCW](#)

40.14.070

- Use of persons, money, or property for private gain [RCW 42.18.217](#)

WASHINGTON ADMINISTRATIVE CODE (WAC)

- Use of state resources- [WAC 292-110-010](#)
- Public records access [WAC 174-276](#) and [WAC 478-276](#)
- Exempt records determination [WAC 174-276-080](#)
- Evergreen Social Contract [WAC 174-121](#)
- Evergreen Student Code of Conduct [WAC 174-120](#)
- Library Access and Use [WAC 174-168-010](#)
- Library Circulation Records [WAC 174-168-070](#)

EVERGREEN POLICIES AND MANUALS

- [Social Contract](#)
- [Student Code of Conduct](#)
- [Ethics](#)
- [DMCA site](#)
- [Union Contract](#)
- [Patriot Act](#)

OTHER

- [Digital Millennium Copyright Act of 1998](#)
- [ALA's intellectual freedom site](#)
- [Executive Ethics Board FAQs](#)
- [ISB Policy on Computer Software Piracy](#)
- [ISB Policy on Public Records Privacy Protection](#)
- [Washington Attorney General's Consumer Protection Division junk email](#)

K20 Network Conditions of Use and Acceptable Use Policies

Approved November 29, 2005
Revised November 14, 2007

[Top](#)