Menu evergreen

Policies

# Appropriate Use of Information Technology Resources

**EFFECTIVE DATE**
January 28, 2025

**CATEGORY**
Administration

**Approval Date:** January 28, 2025

**Steward:** Associate Vice President for Information Technology

**Signature File:** Approval_Form_Appropriate_Use_2025.docx (38.46 KB)

**Previous Version:** Appropriate Use of Information Technology Resources

## 1. Rationale

The College's information technology resources are vital to the work of the entire Evergreen community. Maintaining those resources at a reasonable and dependable level of service requires that each user exercise appropriate and responsible behavior when interacting with the college's systems. Misuse by even a few individuals can disrupt the legitimate academic work of faculty and students, as well as the business and administrative work of the college. This policy is intended to supplement rather than replace the existing laws, regulations, policies and contracts related to the appropriate use of information technology resources.

## 2. Scope

Information Technology (IT) resources are provided by Evergreen for use by its faculty, staff, students, volunteers, and guests. The library provides access to some resources for the public. This policy applies to all users of Information Technology systems and resources. It covers all college owned or managed computer systems, computing-related equipment, college networks, the information stored on any of the above systems, and any other equipment that is connected to the college network, including personally owned devices.

## 3. User Roles and Responsibilities

The individuals using Evergreen's IT resources have a responsibility to protect these resources and respect the rights of others. Users are responsible for familiarizing themselves and using IT resources in accordance with the state and federal laws that pertain to the use of information technology. They are also responsible for familiarizing themselves with this and any other IT-related and ethics policies of the college defining or restricting the use of college property and data. Each individual bears the responsibility for the material they choose to access, store, send or display.

Users should use resources in a manner that does not diminish the reliability or availability of those resources for other users. They should take every precaution to protect the username and password through which they gain access to the network and prevent unauthorized access to their devices and to the IT systems to which they have been given access. They should demonstrate respect for other users' intellectual property, right to privacy, and rights to freedom from intimidation, discrimination and harassment. They should protect college data and ensure that confidential information isn't stored or displayed in unsafe places. They should comply with the security restrictions specific to each system. Everyone is strongly encouraged to make use of an encrypted password manager.

College employees must use college enterprise technologies and devices, when they are provided, for academic work and college business unless an exception is explicitly approved by the Office of Information Technology (OIT) as part of the technology purchasing process. All technology purchases are made by the information technology buyer and subject to college purchasing policies and IT risk assessments. Exceptions

may be allowed for low risk or low impact purchases and are documented in the IT risk assessment and purchasing documents.

*This policy **DOES NOT** prohibit:*

- non-Evergreen devices from being used for college business if they are used to access publicly available college resources. Non-Evergreen devices will not be allowed to connect to the Evergreen Secure Network, thereby restricting the resources that an employee may need to access.
- faculty from following the approved process for procuring and using teaching and learning resources to be used by students in their academic work.

*The policy **DOES** prohibit:*

- Installation of unapproved software and other technologies on a college device.
- Use of unapproved software or technologies with college protected data or for official work functions.

## 4. College Roles and Responsibilities

The college is responsible for practicing good stewardship of state resources. It will treat information about system users in a manner that respects both user privacy and the value of the information. It will take precautions to protect college information systems and the information contained in them from malicious or unauthorized use. It will faithfully execute all IT licensing agreements applicable to college systems. It will respond to lawful requests for disclosure of information.

Pursuant to the policies of the Washington Technology Solutions agency, the college establishes and follows an IT Security Program that implements industry standards and best practices for securing and protecting college data and computing resources.

## 5. Privacy and Public Records

Information system accounts may provide access to sensitive, restricted or confidential data. Users of college information systems will maintain the confidentiality of all data retrieved from them. 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.

Any institutional data not stored in college provided repositories must be stored within an encrypted storage device as approved by the Office of Information Technology (OIT). Unencrypted 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 the secure storage of data should be directed to the Office of Information Technology.

The Family Education Rights and Privacy Act of 1974 governs disclosure of records, documents or other facts containing personally identifiable information about students. All requests for information about students, or requests for lists of individual students, are to be forwarded to the Registrar.

There is no expectation of privacy regarding the use of college technologies or the use of personal technology to conduct college business (e.g. emails, text messages, social media posts, facsimile transmissions, voicemails, and websites visited.) All records related to college business, or created using college technology, may be preserved, collected, and/or disclosed when necessary for legal, operational or management purposes, even if created for personal use.

Other records 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. Disclosure of public records shall be in accordance with WAC 174-276.

# 7. Oversight

The Office of Information Technology will use automated tools to monitor the health of computers, systems, and network infrastructure. Logs or notifications from those tools might indicate issues or activities that need to be further investigated and assessed for the risk they may pose. In those instances, OIT staff will only use enough access to make determinations and correct the issues. The OIT will occasionally change or delete data, files, folders, or email from accounts on college-managed systems in the event of malicious activity, when invited to do so by the owner of the account or are compelled by legal action.

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 or conduct college business; anomalous behavior indicates 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, or it is required by and consistent with legal requirements.

All new employees of the college are to participate in Security Awareness Training as a part of the college required employee policy training. Continuing employees, volunteers, resource faculty, and retired faculty will participate in Security Awareness Training as part of regularly scheduled required employee policy training and as additional security training is made available.

## 8. Personal devices

To protect the security and liability of the Evergreen network, users are required to abide by the following rules when connecting personal devices: computers must have current anti-virus software installed prior to establishing a connection to college resources; users shall not establish networks that bypass Evergreen's security equipment, or install wireless access points, or ad-hoc wireless networks.

Any systems accessed using your personal device and Evergreen account information is to be used for official purposes only and is subject to the same set of responsibilities and restrictions as systems which are accessed using college issued devices.

## 9. College Devices

All software, services and subscriptions to technology services must be approved by the Office of Information Technology before it can be purchased or installed on college devices. This includes both computers and mobile devices. The installation of free, click-thru software application downloads or subscriptions also requires prior approval from the OIT.

All college issued computers and devices must be returned to the issuing office or Technology Support Center upon leaving the college.

## 10. Specifically Prohibited Activities

In the context of the laws, regulations and policies related to using IT resources, the following activities are specifically prohibited:

- sharing your Evergreen passwords
- using your Evergreen password as a password on other systems or services
- sending sensitive information in unencrypted email, messages, or files
- automatically forwarding Evergreen email to external email accounts
- attempting to test security flaws without authorization from the Office of Information Technology
- probing, scanning or reverse engineering any computer or college resource
- using Evergreen systems or networks as a staging ground to illegally access other systems or networks.
- installing invasive software, such as worms or viruses, on any Evergreen system over any network
- altering any data, software, firmware, 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.

The following uses of system resources are also prohibited:

- Using any Evergreen IT resource for unethical purposes, including in support of a private outside business, employment, consulting, or for political purposes (campaigning, soliciting, lobbying, etc. to support or oppose a ballot initiative, or a candidate to public office), unless said use is authorized under the Ethics in Public Service Act or rules of the Executive Ethics Board.
- Using any IT resources for union activities that are not reasonably related to the negotiation and administration of collective bargaining agreements, such as but not limited to union organizing, internal union business, or advocating for a union in a certification, union shop, or other election.
- Using any Evergreen IT resource for committing acts of academic dishonesty (see Student Code of Conduct).
- Booting a college owned device using non-OIT authorized and configured operating systems.
- Installing and/or using software on state-owned equipment which is not directly tied to the academic or administrative work of the college.
- Installing and/or using personal software, games, music, screensavers or other electronic materials which may interfere with the stability or reliability of college owned systems.

- Using software or documentation for any purpose not authorized by the license for that software. Using software or documentation that has been unlawfully acquired, reproduced, distributed, or transmitted.
- Using any IT resource for violating copyright laws (including software, images, music, movies, or text). Any files which are identified as infringement of copyright will be deleted.
- Using an Evergreen IT resource to intentionally disseminate, access, provide a hyperlink to obscenity (as that term is defined in law), or abusive, threatening or harassing messages.
- Using an IT resource to conduct any form of prohibited discrimination as defined in Evergreen's Non-Discrimination Policy.

## 11. Violations

Violations of this policy will be investigated by the college and may result in revocation of access to Evergreen IT resources and/or disciplinary or legal action, potentially including civil or criminal proceedings.

## 12. Policies and Laws Applicable to Information Technology Systems

### United States Code:

- 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
- 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.90.040
- 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 42.17A.315
- Retention of public records – RCW 40.14
- Use of persons, money, or property for private gain – RCW 42.82.160

### Washington Administrative Code (WAC):

- Use of state resources – WAC 292-110-010
- Public records access – WAC 174-276
- Exempt records determination – WAC 174-276-070
- Evergreen Social Contract – WAC 174-121
- Evergreen Student Code of Conduct – WAC 174-123
- 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
- WFSE Union Contract
- Purchasing
- Computer Inventory and Replacement Policy

### Other:

- Digital Millennium Copyright Act of 1998
- ALA's intellectual freedom site
- Executive Ethics Board FAQs
- K20 Network Conditions of Use and Acceptable Use Policies
- Washington Technology Solutions Policies

- College Supported Software

**Tribal Relations, Arts and Cultures**

House of Welcome Cultural Arts Center and The Indigenous Arts Campus at Evergreen.

**Athletics and Recreation**

Get active, build a team and make new friends along the way. Offerings are constantly changing to keep you moving!

**Organic Farm**

A working small-scale USDA-certified organic farm and a learning laboratory for students.

**Lord Mansion and Coach House**

Book your event and enjoy an elegant atmosphere and unique historical connection to Olympia.

INFO FOR

Current Students

Incoming Students

Parents & Families

Faculty & Staff

Donors

Alumni

HELPFUL LINKS

Library

Faculty Directory

Offices & Services

Course Catalog

Academic Calendar

News & Events

Jobs at Evergreen

Report Website Issue

Website Accessibility

Emergency Notifications

Public Records

Policies

Rules Docket

Non-Discrimination Policy

Privacy Notice

Title IX