WALLA WALLA COMMUNITY COLLEGE
INFORMATION RESOURCES ACCEPTABLE USE
ADMINISTRATIVE POLICY 8000

I. POLICY BACKGROUND/PURPOSE

This policy outlines the acceptable use of information resources at Walla Walla Community College (WWCC). The potential for malicious mischief, damage to or loss of equipment or data, and loss of privacy dictate that prudent steps be taken to safeguard the Information Technology Services (ITS) assets of WWCC. The purpose of this policy is to protect the WWCC against internal and/or external exposure of confidential information, malicious activity, including the compromise of systems and services, legal issues, financial loss, and damage to reputation by individuals, either knowingly or unknowingly.

II. AUTHORITY

Board Policy 1370. This policy is a component of the WWCC information security program that is intended to comply with the PCI-DSS, FERPA, Gramm Leach Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), and other regulations.

III. SCOPE OF POLICY

This policy applies to all users of WWCC information technology (IT) resources, including but not limited to employees, students, contractors, consultants, partners, and visitors, including all personnel and affiliated third party contractors. All forms of IT resources, including hardware, software, networks, and data. All data and equipment that is owned or leased by WWCC.

IV. DEFINITIONS

A. De minimis use is brief, infrequent, does not result in additional cost to WWCC, does not interfere with performance of job duties, and does not compromise the security or integrity of state information or software.

V. POLICY

A. It is the responsibility of every user of information resources to know the Information Security Policies and the acceptable use of information resources, and to conduct their activities accordingly.

B. Personnel using data and information resources must use them for business purposes in accordance with their job functions and responsibilities, serving the interests of WWCC and its customers in a legal, ethical, responsible, and secure manner, with respect for the rights of others. Information Resources, including, but not limited to:
   1. Internet/Intranet/Extranet-Related and Core Systems
   2. Computer Equipment
   3. Software
   4. Operating Systems
   5. Storage Media
   6. Network Accounts Providing Electronic Messaging

C. Notice of Breach of information
   1. Notification to affected individuals of an information breach or compromise must be made in the most expedient time as outlined in RCW 42.56.590.

2. Notification of an information breach or compromise must be made in the most expedient time possible to your Supervisor and ITS.
3. WWCC will not be responsible for any breach/compromise of data outside of the framework of this policy and user's work responsibilities.

D. General Use
1. Safeguard user accounts and passwords, use them only as authorized.
2. It is the responsibility of the user to know, understand, and abide by all licensing agreements of software utilized. See EDUCOM Code (http://www.educause.edu/ir/library/html/code.html) for more information and to review the policy.
3. Unauthorized copying of software is illegal. Copyright laws protect software authors and publishers
4. To accommodate users, WWCC understands users will access the internet for personal needs as long as it is de minimis (trivial or minor) usage.
5. It is expected that users will exercise good judgement regarding de minimis personal use of state resources and any question regarding appropriate use will be decided by Human Resources.
6. Notify the ITS of any suspected or actual security violations/incidents.
7. Secure all unattended workstations from unauthorized viewing or use.
8. All workstations must be configured to automatically lock after 15 minutes of inactivity and users should log off or lock their machines during extended periods of inactivity.

E. Unacceptable Use

The following unacceptable activities are by no means exhaustive, but attempt to provide for activities that are strictly prohibited:

1. Damaging computer systems intentionally or unintentionally.
2. Preventing another user from authorized resources.
3. Accessing unauthorized systems or data resources, or using functions that are not necessary for the performance of the user's job duties.
4. Revealing account passwords to others. Users who receive usernames and passwords must keep their usernames and passwords confidential and must not share that information with others including ITS staff.
5. Using another person's account, with or without their permission.
6. Providing information about employees to parties outside WWCC.
7. Providing protected customer and/or vendor information to any unauthorized person.
8. Intentionally corrupting, misusing, or stealing software or any other computing resource.
9. Sending unsolicited (spam) electronic messaging (e.g. email, teams chats) and chain letters.
10. Forging electronic message header information.
11. Using electronic messaging, telephone, or other communication methods, to actively engage in procuring, viewing, or transmitting material that is in violation of sexual harassment or hostile environment laws.
12. Accessing, editing, deleting, copying, or forwarding files or communications of another user in any media (e.g. paper or electronic) unless assigned as a job requirement or with prior consent from the file owner.

13. Deleting, editing, or copying files in another person's computer or electronic messaging account.
14. Illegal use, including duplication or distribution of copyrighted or WWCC proprietary material, including electronic, hardcopy, audio, and video in any medium.
15. Procurement or use of any Software as a Service (SaaS) providers without the approval of ITS.
16. Implementation of any information technology component, product, or service associated with WWCC without the approval of ITS.
17. Unauthorized system modifications are prohibited. Such restrictions are designed to ensure system integrity and security. These include but are not limited to the following:
    i. Unauthorized installation/removal of hardware and/or software.
    ii. Unauthorized access into network and/or system resources.
    iii. Deliberate introduction of invasive computer software such as viruses.
    iv. Changes to system security settings.
18. Using WWCC resources for personal business transactions.
19. Knowingly executing a program, without prior authorization from ITS.
20. Operating a wireless network or allowing other computers to connect to your computer wirelessly, without prior authorization from ITS.
21. Users must not reveal any information about the WWCC's students, clients, or employees which is not already publicly available without expressed written permission from WWCC.
22. Disclosure of Personally Identifiable Information (PII) such as social security numbers, bank/credit card numbers, driver's license/id numbers, etc. and any other information classified as confidential, personal, or sensitive to any unauthorized persons, unless there is a legal or regulatory requirement. All such information must be approved WWCC.
23. Unencrypted transmission of PII, trade secrets, proprietary financial information and financial account numbers such as in the body of or an attachment to an electronic message (e.g. email and instant messaging), via FTP, or via fax.
24. Storing confidential information including PII (and confidential, personal, and sensitive information), trade secrets, proprietary financial information, or financial account numbers on any unencrypted devices including desktops, laptops, USB devices, and mobile computing devices.
25. Users should not open any electronic message attachment that are not expected, or from unknown addresses or contacts, or appear in any way suspicious.
26. Users must not use WWCC accounts to post publicly accessible messages or posts.
27. Users shall not perform vulnerability scans, monitor network traffic, or attempt to elevate rights or privileges to gain access to information not expressly intended for their use, without formal approval from ITS.

F. Other Provisions
1. Authentication is required in order to use any technology.
2. Accessing unauthorized systems or data resources, or utilizing functions that are not necessary for the performance of the employee's duties.
3. Users are responsible for checking policies and procedures whenever changes are announced or when they return from an extended leave. Users acknowledge that the WWCC accepts no responsibility or liability for the specific acts of individuals that violate this or any applicable law, policy or procedure.

G. Exceptions
    1. Only the President of WWCC or a designated appointee is authorized to grant exceptions to this policy.

V. COMPLIANCE

To ensure compliance with this policy, WWCC may perform periodic monitoring of systems, networks, and associated equipment at any time. Personnel using any WWCC information resources, consent to disclosing the contents of any files or information stored or passed-through WWCC's network and may be subject to monitoring.

A. Enforcement
    1. Personnel and students using WWCC's information resources in opposition to this policy may be subject to limitations on the use of these resources, suspension of privileges (including internet access), as well as disciplinary and/or legal action, including termination of employment, or suspension of enrollment.
    2. Employees, contractors, consultants, temporaries, partners, and all personnel affiliated via third parties shall sign an agreement to comply and be governed by this policy and the WWCC Information Security Policies upon hire and must be reviewed annually.

B. Violations
    1. In conjunction with the Vice President of Human Resources, a Supervisor, Department Supervisor, Dean, or Vice President will address employee violations of this policy.
    2. The Vice President of Student Services will address student violations of this policy in accordance with the Student Code of Conduct.

Policy Contact: Vice President of Administrative Services
Approved by (Department/Body): Dr. Chad Hickox, President
Date Originally Approved: November 19, 2003
Last Reviewed/Revised on: September 7, 2023