

Wor-Wic Community College Computer Usage Policies & Procedures

This policy outlines the acceptable uses of and the limitations, responsibilities, and obligations for using Wor-Wic Community College's computing and information technology resources (computer resources). Computer resources include, but are not limited to, equipment, software, e-mail, networks, data, and telecommunications equipment whether owned, leased, or otherwise provided by the college. Wor-Wic provides access to computer resources to support the educational mission of the college. The granting of the privilege to use these resources is predicated on the user's acceptance of and adherence to the corresponding conditions and user responsibilities detailed in this policy.

The college reserves the right to limit or extend access to computer resources. The college reserves the right to collect, process, and retain appropriate information pertaining to the user's usage and the integrity and security of its computing resources. Disciplinary sanctions for violations range from the loss of computer use privileges, dismissal from the college, and/or legal action, depending on the nature of the violation. In the event of a law enforcement investigation with a subpoena (police, FBI, DEA, etc.), the college reserves the right to provide the requested access/information.

All computer users are expected to act responsibly, ethically, and legally, and to limit their use of computer resources to the educational purposes and legitimate business of the college. The college will not be held liable for the actions of college computer users when those actions are inconsistent with these policies and procedures. The college makes no representations concerning the availability of computer resources, the privacy of material, and the integrity or accessibility of material placed on these resources. The college is not responsible for any damages resulting from the receipt and/or transmission of any electronic information.

Computer usage policy violations include:

1. Unauthorized use of a computer;
2. Obstructing the operation of the college's computer resources, including, but not limited to, intentionally damaging equipment, tampering with cables, adding or deleting files or software without authorization, changing network settings, and the introduction or creation of invasive software, such as worms, or viruses, Trojan horses, e-mail bombs, etc.;
3. Violating the privacy of individuals, including viewing, monitoring, copying, altering, or destroying any file, data, transmission (e.g. network packets), or communication without permission from the owner;
4. Mimicking, replacing, or disrupting services used by Wor-Wic to maintain the network, including, but not limited to, DNS, DHCP, BOOTP, WINS, or any other server that manages network addresses;
5. Computer Services has the sole authority to assign host names and network addresses to computers attached to the college's network. Thus, a user may not manually configure his/her computer to use a host name, network address, or hardware address that is not defined by Computer Services for their use;
6. No network devices may be attached to the college's network without Computer Services' approval. This includes, but is not limited to, hubs, switches, wireless access points, routers, or similar devices;
7. Researching or attempting to defeat computer and network security measures, implementing self-replicating codes, possessing "cracker tools", as well as intentionally developing and/or using programs that are designed to harass other network users, bypassing system security mechanisms, stealing or "cracking" passwords or data sets, denying access or otherwise interfering with system services, replicating themselves or attaching themselves to other programs, or evading software licensing or copying restrictions;
8. Violation of copyright laws, including the use of images, programs, sounds, and text;
9. Use of computers to send or receive electronic mail of an unwanted, abusive, threatening, obscene, slanderous, or harassing nature;
10. Displaying on a computer screen or printing materials of a sexually-explicit or discriminatory nature;
11. Monopolizing computer systems, overloading networks with excessive data or wasting computer time, disk space, printer paper, or other college resources;
12. Unauthorized use of college computers for commercial, political or religious purposes, personal profit, the promotion of other external organizations, or other activities not related to the mission of the college;
13. Use of computers to violate any other college policy or procedure or for illegal or criminal purposes that violate federal, state, and local laws; and
14. Violation of any additional rules or regulations regarding computer usage established by authorized college employees.

Violators are subject to college disciplinary procedures. Based on the nature of the offense and/or the number of violations, employees are subject to appropriate personnel action, up to and including dismissal. Students are subject to disciplinary action taken in accordance with procedures that govern student conduct, up to and including permanent suspension. If appropriate, the college may pursue criminal and civil prosecution.