

**Southern Maine Community College**  
**Student Computer & Network Usage Policy**  
(excerpted from the Compass)

---

**Introduction**

This policy governs all uses by students of the computing resources maintained by Southern Maine Community College and is designed to protect both the students and the College's computing resources which include, but are not limited to, computers, peripherals, network components, and the physical and logical data. Each student who uses College computer resources is responsible for reading, understanding and complying with this policy.

**Guidelines**

- Use the College's website, server, and all other related computer equipment and services only for academic, educational, or professional purposes, which are directly related to official College business and in support of the College's mission. Be responsible for all activities conducted using SMCC user IDs.
- Do not disclose SMCC user IDs or passwords to anyone.
- Access only SMCC files and data that are your own, that are publicly available, or to which you have authorized access. Be considerate in your use of shared resources and refrain from monopolizing systems, overloading networks with excessive data, or wasting computer time, disk space, printer paper, manuals or other resources. If it is necessary to allow an authorized third person to access a user's files or data, as in the case of illness, a formal request must be made in writing to the Dean of Students.
- Student user accounts and all data found in student user accounts may be removed at the end of each semester.

The Following are Prohibited:

- Use of another person's user ID or password.
- Use of another person's files or data without permission.
- Unauthorized interception, reading, copying or modifying of private electronic data.

- Use of computer programs to decode passwords or access controlled information.
- To view, download, store, or transmit materials that, if viewed in public, may create a hostile environment and constitute sexual harassment under the SMCC policy or the law.
- To circumvent, subvert, or attempt to circumvent or subvert system or network security measures.
- To purposely engage in any activity that might be harmful to system/network or to any information stored thereon, such as creating or propagating viruses, disrupting services, or damaging files.
- To download any on-line software without authorization from the IT Staff.
- To use the network for purposes that places a heavy load on scarce resources.
- To use Southern Maine Community College's computers or networks to libel, slander, or harass any other person. The following shall constitute computer harassment: (1) Using the computer to annoy, harass, terrify, intimidate, threaten, offend or bother another person by conveying obscene language, pictures, or other materials or threats of bodily harm to the recipient or the recipient's immediate family; (2) Using the computer to contact another person repeatedly once the recipient has provided reasonable notice that he or she desires such communication to cease; (3) Using the computer to disrupt or damage the academic research, administrative, or related pursuits of another; (4) Using the computer to invade the privacy, academic or otherwise, of another or threatened invasion of privacy of another.
- To waste computer resources, for example, by intentionally placing a program in an endless loop or by printing excessive amounts of paper.
- To use the College's systems or networks for personal gain; for example, by selling access to your user ID or to College systems or networks, or by performing work for profit with College resources in a manner not authorized by the College.
- To use the College's systems or networks to transmit any material in violation of United States or Maine laws or regulations.
- To engage in any other activity that does not comply with these Guidelines presented above.

## **Privacy**

Users of the College's Computer Network System should have no expectation of privacy over any content, communications, transmissions, or work performed thereon. Computers owned by the College are provided for college and educational use only. Note that the College retains ownership of all computer transactions as business records and these records may be subject to discovery in litigation. Any information on a College computer or storage media may be subject to the State's public record law and may therefore be subject to disclosure upon request.

The College does not routinely monitor students' computer activities unless it receives notice of possible misuse or violation of policy. However, should the College discover, as a result of routine maintenance, technical fault or investigation of criminal activity, misuse or violation of policy, it will not guarantee privacy. By using computers on campus, students are waiving their right to privacy and are consenting to College review and monitoring of their computer use.

**Further:**

- The College endeavors to maintain the privacy of personal communications. Where necessary, the College will take action to protect the integrity and operation of its networks.
- In the course of routine system maintenance, technical problems, investigation of an alleged violation of policy, or criminal investigations, College employees will be permitted to intercept, read, copy or modify private electronic data, either in transit across a network or stored within a computer system.
- The College will collect utilization statistics based upon network protocol and application use.
- The College will progressively restrict non-essential users where network utilization results in performance degradation. Such restriction will be publicized to users through appropriate means.