

St. Mary's College of Maryland Computer Use Policies

Ethics of Computer Usage

The computer facilities at St. Mary's College of Maryland (SMCM) provide a vital service to the entire campus community. Adherence to certain rules of courtesy and ethics is essential to maintaining the integrity of our computer systems. SMCM considers it a serious offense for any user to attempt to degrade the performance of the system, to seek to penetrate computer security, or, in any way, deprive or attempt to deprive other users of resources or access to the computer facilities. In short, we ask all users to refrain from abusing their computer privileges.

The following activities are examples of violations of courteous and ethical conduct:

- Altering the equipment or modifying the operations of any College equipment;
- INSPECTING, modifying, or copying data or programs without authorization from the owner;
- Using the electronic mail system to send abusive, obscene, or otherwise harassing communications;
- Using the computer system for commercial purposes;
- Specifying false or misleading identification when required to do so for any purpose associated with the use of the computer system;
- Attempting to penetrate or alter computer security mechanisms or gain access to restricted information;
- Using another person's account;
- Failing to turn over an old device when issued the replacement or at the end of a loan period
- Engaging in any activity which deprives others of their privileges on the computer system.

There are two additional important considerations:

1. Files stored on the SMCM network drive or cloud storage are subject to monitoring and may be subject to examination by the system administrator if evidence exists that such an intrusion is warranted.
2. Users are reminded that data is collected daily which permits the analysis and accounting of the system's use. While the assimilation of this data is not routinely announced to users, no attempt is made to conceal the fact of their collection. Please see our AI policy on how data collected may be used by AI engines.

3. Users are responsible for backing up their files on their individual machines. The Office of Information Technology will recommend a backup strategy at the issuance of your machine.
4. The Office of Information Technology employs tools to monitor and prevent cybersecurity risks. Individuals who are contacted as a result of a flag from such a system must respond and cooperate with technician intervention.

The above is a statement on the ethics of computer use and constitutes the policy of SMCM. All users of the SMCM computer facilities are responsible for understanding these principles. SMCM reserves the right to deny access to any account, without prior notice. Anyone violating these principles will have their access revoked and be reported to the relevant authorities.

Data Privacy and Appropriate Use

SMCM has an Office of Information Technology (OIT) which includes data that is needed to conduct the business of the College. The College endeavors to maintain the security of the system, and to provide employees with information on a need-to-know-only basis. However, employees should be aware that some personal information, such as Social Security number, home address, and phone number may be viewed by college employees or other authorized system users in the course of conducting College business. Inappropriate and unauthorized use of such information includes use of that information for non-College business purposes or passing information to another college employee who does not have the need to know or to any person outside the college who does not have a right to know. Unauthorized use of another's personal or proprietary information will result in disciplinary action, which may include termination of employment.

Anyone with a question about this policy or concerns about unauthorized use of confidential data should contact the Office of Human Resources, who is charged with monitoring compliance.

I hereby acknowledge receipt of these SMCM Computer Usage Policies and agree to comply with them.

Signature: _____ **Date:** _____

Print Name: _____