

Acceptable Use Policy for Information Technology Resources

1. Purpose and Scope

County College of Morris (“the College”) is dedicated to advancing learning, teaching, and official College business through the responsible use of information technology resources. This Acceptable Use Policy (“Policy”) outlines the standards for acceptable and responsible use of computers, networks, and technology equipment by students, faculty, staff, and authorized community members. Adherence to these guidelines ensures equitable access, security, and legal compliance for all users.

2. Access and Privileges

1. Access to information technology resources is granted as a privilege to support academic study, instruction, official College business, and authorized College activities.
2. All users are expected to act responsibly and ethically, understanding that access is conditioned upon compliance with this Policy and applicable laws.
3. Resource availability may change due to evolving technology and demand; users must recognize that acceptable use determinations may be updated as needed.

3. Priority and Restricted Use

1. Classrooms, laboratories, the Learning Resource Center and general campus computing facilities prioritize academic and instructional activities.
2. Certain computers and maybe designated for specific applications. The college will provide notice where use is restricted.
3. Recreational use of computers is only permitted on equipment specifically designated for open access, and not in classrooms or labs.

4. Privacy and Public Records

1. The College is obligated to comply with public records laws. All data residing on College networks or devices may be considered public records and subject to e-discovery and public disclosure, unless exempted by law (see N.J.S. 47:1A-1.1).
2. The College places a high value on privacy and recognizes its critical importance in an academic setting. In limited circumstances, including but not limited to technical issues or failures, law enforcement requests, or government regulations, the College may determine that other interests outweigh the value of a user’s privacy expectation. Thus, no user should expect privacy regarding the use of College information technology resources. This includes, but is not limited to, email, voicemail, and files stored on College systems. Procedural safeguards have been established to ensure access is attained only when appropriate.
 - a. **Conditions:** In accordance with state and federal law, the College may access all aspects of IT Systems, without the consent of the user, in the following circumstances:

- i. When necessary to identify or diagnose systems or security vulnerabilities and problems, or otherwise preserve the integrity of the College's IT Systems;
 - ii. When required by federal, state, or local law or administrative rules;
 - iii. When there are reasonable grounds to believe that a violation of law or a significant breach of College policy or procedure may have taken place, and access and inspection or monitoring may produce evidence related to the misconduct;
 - iv. When such access to the IT/Enterprise Applications Systems is required to carry out essential business functions of the College; and
 - v. When required to preserve public health and safety.
3. Communications originating from or delivered to College accounts may be preserved as part of the public record and used for disciplinary or legal purposes.

3. Communications originating from or delivered to College accounts may be preserved as part of the public record and used for disciplinary or legal purposes.

5. Guidelines for Acceptable Use All users must:

1. Use College information technology resources primarily for academic study, instruction, official College business, or authorized activities.
2. Respect the integrity and security of computer systems, networks, and data.
3. Ensure compliance with software licensing agreements.
4. Safeguard their account credentials and not share passwords with others.
5. Refrain from accessing, copying, or modifying files or accounts belonging to other users without authorization.
6. Abide by federal, state, and local laws and regulations related to digital information and technology.

6. Prohibited Activities

The following activities are strictly prohibited. This list includes but is not limited to:

1. Engaging in illegal activities or actions that threaten the safety of people or security of equipment.
2. Intentional damage, destruction, or unauthorized modification of equipment, software, or data.
3. Violating system security protocols or attempting unauthorized access to College or third-party systems.
4. Simultaneously logging in from multiple locations using the same account credentials.
5. Eating or drinking in public computing facilities where prohibited.
6. Using College resources for personal business or commercial purposes without prior approval.
7. Plagiarism, cheating, or other forms of academic dishonesty involving information technology.
8. Unauthorized copying, downloading, or sharing of copyrighted material.
9. Libel, slander, harassment, or threats via electronic communications.

10. Sending forged, spam, or disruptive communications that interfere with system performance.
11. Spreading computer viruses, worms, or making unauthorized network entries.
12. Sharing account passwords with others.

7. Enforcement and Violations

1. Alleged policy violations will be reviewed individually.
2. Consequences for violations may be; loss of access to email, computer systems, network privileges, and referral to appropriate College or legal authorities for further action.
3. The College reserves the right to update, modify, or make determinations regarding the appropriate use of technology resources as technologies and community needs evolve.

8. Acknowledgment and Updates

1. Continued use of College information technology resources indicates acceptance of and agreement to comply with this Policy.
2. This Policy may be revised periodically; users are responsible for reviewing and adhering to the most current version as posted by the College.