Georgia Military College Computer Ethics and Guidelines

General Statement

This document provides guidelines for the acceptable and ethical use of the computers, networks and related services at Georgia Military College. These guidelines have been developed to ensure a quality computing environment at GMC that furthers the academic and service mission of the institution. Providing this environment requires equitable resource distribution, computer and network availability, personal privacy, and data integrity. Achieving this goal requires that everyone in the College community cooperate and adhere to these guidelines.

Georgia Military College acquires, develops, and maintains computers, computer networks, and other information technology resources. These resources are intended for direct and indirect support of the college's instruction, research, and service missions; of the college's administrative functions; and of student and campus life activities. Access to these resources, whether from on-campus or from a remote location, is a privilege and is subject to the applicable laws and policies and the highest standards of ethical behavior. Particular uses of any of these resources are not made legitimate simply because those uses may be technologically possible. Users must abide by all applicable restrictions imposed by these guidelines. In addition, student users must abide by the provisions of GMC Honor Code.

Security

Georgia Military College employs various measures to protect the security of its computing resources, user accounts, and data by storing all sensitive user data in secure and protected locations. Transmission of sensitive data is also encrypted across all forms of network traffic to ensure the information is not captured by a third party. Users must engage in safe computing practices by establishing appropriate access restrictions for their accounts (usernames and passwords), safeguarding passwords, changing passwords regularly, and promptly reporting any misuse or violations of this policy.

Privacy

Users should also be aware that their uses of college computing and technology resources are not private. The normal operation and maintenance of these resources require the backup of data and communication records, the logging of activity, the monitoring of general usage patterns, and other activities necessary for the provision of service. The system administrator and his or her designees have access to all data and information (e.g., e-mail messages, files, etc.) of any user; however access to protected information is controlled and access is granted on an as-needed basis to authenticated college personnel. Although Georgia Military College does not permit the casual inspection of files, the college reserves the right to monitor and disclose the contents of e-mail messages and other files under appropriate circumstances. Also, under the Georgia Open Records Law, it is possible that information which is stored on a computer system, including electronic mail, would be available for inspection by any member of the public.

Individual Responsibilities

Each user of Georgia Military College computer and information technology resources is expected to accept and comply with the following responsibilities:

1. Use only those resources which s/he is authorized to use. Accounts and passwords may not be shared with, or used by, persons other than those to whom they have been assigned by the college. Unauthorized access to another user's account or providing your username and password to another person will be grounds for appropriate sanctions. Georgia Military College reserves the right to suspend misused accounts indefinitely.

2. Use computer and information technology resources only for their intended purpose. Georgia Military College's computing and information technology resources, facilities, and services are to be used for purposes congruent with the college's educational mission. They may not be used for commercial, or political activities, charitable solicitations, and other such uses, unless expressly authorized by the Vice President of Information Technology.

3. Respect the rights and privacy of others. Ability to gain access to another person's account does not imply authorization to do so. Interference with the ability of other users to make appropriate use of the resources is prohibited. The systems and services may not be used to harass, discriminate against, defame, or invade the privacy of others.

4. Protect the integrity and security of the computer and information technology resources. Acts which are intended to damage computing resources, to deny service to other users, gain privileged access to secured data, or to compromise the integrity of the security systems are prohibited. Any user who is found to be attempting any of the above actions will be subject the maximum penalty given by Georgia Military College and, if applicable, will be prosecuted to the furthest extent of the applicable laws.

5. Protect the integrity and security of sensitive and confidential data. Student or employee confidential data must not be stored on campus or home computers for security purposes. Protected data includes, but is not limited to, Social Security Numbers, birth dates, credit card numbers, and student information protected by the Family Educational Rights and Privacy Act (FERPA).

6. Protect the computing networks by not authenticating into a workstation and then leaving that workstation unattended. All workstations that are unattended should be locked.

7. Respect the finite capacity of college computing and network resources. Users are expected to respect the finite capacity of college computing and network resources and to limit use to a reasonable amount as determined by the Office of Information Technology. If an individual's use is interfering unreasonably with the activity of others, the college may require that person to limit or refrain from specific uses.

8. Abide by copyright laws and policies. Users must abide by all applicable laws and college policies (e.g., Copyright, Intellectual Property) to protect the copyrights and intellectual property rights of others. Copyrighted works may include texts, cartoons, articles, photographs, songs, software, graphics, and other materials. Users should be aware that many materials available through the Web are protected by copyright. It is the responsibility of the user to assume that materials found on the Web are copyrighted unless the materials contain an express disclaimer to the contrary. Users must obtain permission of the creator or publisher to copy or use software or other copyrighted materials written or created by others, and must abide by contracts and agreements controlling installation and use of such software and other materials.

9. Users are not permitted to provide network or computer-based services using Georgia Military College computers or networks without prior permission from the Office of Information Technology. Examples of such services include, but are not limited to, file transfer protocol (FTP) and WEB servers.

10. Because access to the Internet provides connections to other computer systems located all over the world, users (and parents of users, if the user is under 18 years old) must understand that Georgia Military College does not control the content of the information available on these other systems. Some of the information available is controversial and, sometimes, offensive. School employees, students and parents of students must be aware that access to the Internet will be withdrawn from users who do not respect the rights of others or do not follow the rules and regulations established by Georgia Military College.

11. The use of File Sharing services or Peer-to-Peer networks is strictly prohibited on the Georgia Military College network or computing resources. Users who are found to use any of the above mentioned may have computing access suspended and may be subject to disciplinary action.

12. When browsing the internet, users must not access materials that are deemed indecent, pornographic, profane or violent. Access to such material is strictly prohibited. Any users found to have accessed inappropriate website may be subject to termination or expulsion.

13. Users of Georgia Military College’s computing systems must use the system in an ethical and legal manner and in accordance with Georgia Military College's policies and procedures. Usage of the system to harass, defame, or invade the privacy of others, or to send or receive obscene materials, is not allowed and may result in disciplinary action or prosecution under applicable federal or state statutes.

Social Media

1. Users are personally responsible for the content they publish on-line, whether in a blog, social computing site or any other form of user-generated media. Be mindful that what you publish will be public for a long time. Protect your privacy and take care to understand a site's terms of service.

2. Identify yourself and, when relevant, your role at Georgia Military College when you discuss the College or College-related matters. You must make it clear that you are speaking for yourself and not on behalf of Georgia Military College unless granted specific authority to do so.

3. If you publish content online relevant to Georgia Military College in your personal capacity use a disclaimer such as this: "The postings on this site are my own and do not represent Georgia Military College's opinions."

4. Respect copyright and fair use laws.

5. Do not disclose Georgia Military College's or another's confidential or other proprietary information.

6. Respect your audience. Respect privacy. Don't use ethnic slurs, personal insults, obscenity, or engage in online conduct that would not be acceptable in Georgia Military College’s workplace.

Legal Restraints

Users of GMC computing facilities are expected to abide by State and Federal laws that apply to the usage of computers. These laws exist to “establish certain acts involving computer fraud or abuse as crimes punishable by defined fines or imprisonment or both”. As an example, the Georgia Computer Systems Protection Act was enacted in 1991 to “provide for criminal liability and definition of penalties for the crimes of computer theft, computer trespass, and computer invasion of privacy, computer forgery, and computer password disclosure”. The penalties range from fines up to $50,000 and imprisonment up to 15 years. The full text of this act and others are available via the World Wide Web.