COMPUTING FACILITIES

The guidelines that follow are designed to govern the use of college computing facilities and apply to all students and employees. The term "computing facilities" is used in this context to include any computer, printer, network component, or other related resource belonging to or provided by the college and applies whether a user is at the college, their home, or any other location. Willful violation of these guidelines will be treated as misconduct and may result in disciplinary action, including denial of access to computing facilities.

General:

1. Computing facilities are provided to students and employees by the college in order to support the mission of the college.
2. Student access is provided for use in association with a course of study and activities related to that course of study.
3. Employee access is provided for use in association with college duties.
4. All who use the college computing facilities agree to do so in a manner that is ethical and legal and does not interfere with others.

Restrictions:

1. Use of college computer facilities for non-college-related tasks is not permitted.
2. You may only use facilities that have been authorized for your use. If access is protected by a password, you are not to make this password available to others. You may not use any account set up for another user, nor may you attempt to discover the password of another user.
3. You may only use authorized facilities for authorized purposes. For example, facilities made available for teaching may not be used for private gain.
4. You must be aware of the laws related to software copyrights and licensing. Software must not be copied except with the expressed permission of the copyright holder.
5. You may not attempt to copy information belonging to other users without their expressed permission.
6. You may not attempt to interfere with the operation of the college's computing facilities.
7. You may not attempt to circumvent the security of any of the college's computing facilities.
8. You may not connect a privately owned computer or network equipment to the Greenville Technical College network.
9. You may not use the college's computing facilities or networks to send, receive, or access material that is deemed to be obscene, offensive, or harassing to others. The college reserves the right to determine if a particular source of information may contain such material and to restrict or deny access to such sources at its discretion.
10. To ensure the quality and standardization of services, only authorized personnel are allowed to repair, upgrade, install, and configure computer and network equipment. Therefore, students or employees are not allowed to (1) open or disassemble computer equipment for any reason; (2) connect or disconnect computer or network equipment from the campus network, or (3) move computer equipment without notifying "MOVERS" by email.
11. To maintain standardization of equipment, parts, and services, employees shall follow all state and institutional procurement standards. Employees shall not purchase computer equipment on GTC credit cards and/or use personal funds to circumvent the system. If you need assistance with new equipment, parts, or services, click the OIT Help icon installed on all employee GTC desktop computers.

Other:

1. The college makes computing facilities consisting of hardware and software available to internal and external users. The college accepts no responsibility for any damage to or loss of data arising directly or indirectly from the use of these facilities or for any consequential loss or damage. The college makes no warranty, expressed or implied, regarding the computing services offered or their fitness for any particular purpose. The college's liability in the event of any loss or damage shall be limited to the fees and charges paid to the college for the use of the computing facilities which resulted in the loss or damage.
2. The college provides no facilities that guarantee the confidentiality of files. The computer systems administrator and his or her designee may have the ability to view all messages and files of any user; however, it is not the routine policy of the administrator to view such files. The intention is to keep files private, even though such privacy cannot be guaranteed.