

Waycross College

Campus Network and Computer Acceptable Use Policy [A.U.P.]

Effective Date: March 31, 2007
Last Revised: December 15, 2006

Status:

- Draft
- Approved

Responsible University Officer
Director of Computer Services

Responsible Coordinating Office
Computer Services

Online Publication
<http://www.waycross.edu/compserv/itpolicy/>

1. Purpose

This policy outlines the acceptable use and protection of Waycross College information technology resources by employees, students, and visitors. Access to networks and computer systems owned by Waycross College is a privilege, not a right, and implies user responsibilities. Such access is subject to Waycross College policies, standards, and procedures; and federal, state, and local laws.

2. Scope

This College-wide policy addresses proper use of all Waycross College computing and network resources, including proper management of those resources. This policy applies to use of the Waycross College network regardless of ownership of the device(s) connected to the network. This policy is the governing information technology policy for Waycross College whenever a policy conflict occurs. Other policies, standards, and procedures may supplement security restrictions, but may not relax the minimum requirements in this policy.

3. Policy

Waycross College provides information technology resources for the purpose of transacting official business of Waycross College. The Board of Regents and Waycross College establish acceptable use guidelines for the proper use of these resources.

3.1. Responsibilities of Information Technology Users

3.1.1. Privacy

In accordance with BOR policies regarding the use of State resources, users should have no expectation of privacy when using Waycross College computing resources. Waycross College computers and campus network are publicly owned and may be subject to the Georgia Open Records Act, including the data and files that are stored on the computers or traverse the network. Computer Services monitors network traffic in aggregate data. Computer Services may investigate network traffic and / or computer resources further if a network problem, traffic anomaly, or policy violation exists.

3.1.2. Intellectual works and copyrights

Users are prohibited from unlawfully installing, using, inspecting, copying, storing, or distributing copyright-protected material (e.g. computer programs, movies, television programs, music) on Waycross College owned systems or on the Waycross College network.

Users creating intellectual works using Waycross College computers or campus network, including but not limited to software, should consult Determination of Rights and Equities in Intellectual Property (refer to Board of Regents Policy Manual, section 603.03, 2/2/94 and any subsequent revisions at <http://www.usg.edu/regents/policymanual/600.phtml>).

Use of any peer to peer applications (such as downloading of movies, music, or other copyrighted material) by faculty, staff, or students is prohibited on any college-owned computer system or via the college network. If a faculty member, staff member, or student feels they have a legal, legitimate reason to use such an application, the individual must obtain prior approval from the Director of Computer Services.

Students are prohibited from hosting files for access via peer to peer applications while connected to the student wireless network provided by Waycross College. If an application resident on a student's computer cannot be configured to disable the hosting of files on peer to peer networks, the software must be removed from the computer or the computer must not be used on the student wireless network. It is the sole responsibility of the student to disable file hosting via peer to peer applications prior to connecting to the student wireless network provided by Waycross College.

3.1.3. Data confidentiality and integrity

Users are responsible for upholding the confidentiality and integrity of data. Users are prohibited from inspecting, copying, altering, or destroying anyone else's files without proper authorization.

3.1.4. Responsible use of resources

Users must ensure that Waycross College computer systems and network resources are used for scholarly or business purposes only. Incidental personal use is permissible if the use meets the following standards:

- Does not create a security or legal risk for Waycross College
- Does not interfere with worker productivity
- Does not consume more than a trivial amount of resources that could otherwise be used for scholarly or business purposes
- Does not require the installation of any software or hardware unrelated to business or scholarly use
- Does not constitute inappropriate behavior for a professional work environment

3.1.5. Networking implementation and management

Computer Services is solely responsible for planning, implementing, and managing the Waycross College network, including wireless connections. The following technologies are only to be implemented at Waycross College by Computer Services: routers, switches, hubs, wireless access points, and other networking technologies.

3.1.6. Software installation and maintenance

Computer Services is solely responsible for the installation and maintenance of software on Waycross College computers. Faculty, staff, and students are prohibited from installing, modifying (other than general user settings), or removing software on Waycross College computers. All requests for software installation or maintenance should come through the Computer Services online work order system. In rare cases Computer Services may grant permission for a faculty member, staff member, or third party, under the supervision of a Computer Services staff member, to install or modify software on a Waycross College computer.

3.1.7. Software Inventory

Computer Services maintains an inventory of software installed on Waycross College computers. The purpose of the inventory is to ensure that Waycross College does not violate the software copyright licenses of software installed on Waycross College computers. The inventory is updated when computers are set up, updated, or decommissioned.

Periodic software inventories are also performed by Computer Services staff. The privacy of the user will be respected as far as possible while performing the software inventory. If software license violations or prohibited software is found during the inventory process, the Director of Computer Services will be notified and take appropriate action. Unlicensed software, or software used outside of its legal license restrictions, and prohibited software will be removed from Waycross College computers. If Computer Services becomes aware of additional policy violations during the course of periodic software inventories the Director of Computer Services, or his designate, will notify the appropriate supervisor. In the event a software license violation or policy violation appears to be a personnel matter, the Director of Computer Services will notify the Vice President of Business Affairs.

3.1.8. Use of personally-owned systems and equipment

Personally owned systems and equipment may not be connected to the Waycross College network or Waycross College computers without the prior approval of the Director of Computer Services. If such approval is granted, authorized users have a responsibility to ensure the security

and integrity of personally owned (or managed) systems and equipment, as well as data accessed through such systems.

Any connection to the Waycross College network is subject to the policies of Waycross College and may be terminated without notice for violation of policy.

3.1.9. Security responsibilities

Authorized users are individually responsible and accountable for any use of their account and password. These passwords should not be shared under any circumstances.

Authorized users may have access to privileged information that must be protected. In receiving access to this information, authorized users accept responsibility to protect the information accessed and used on their computer.

3.1.10. Attempts to circumvent security

Users are prohibited from attempting to circumvent or subvert any system's security measures. This does not preclude the use of security tools by appropriately authorized personnel. While the following list provides examples of disallowed practices, it is not a comprehensive list and is intended to only provide examples:

- Password decrypting or cracking tools
- Denial of service (DoS) or distributed denial of service (DDoS)
- Harmful activities (e.g. IP spoofing, port scanning, disrupting services, damaging files, or intentional destruction of or damage to equipment, software, or data)
- Unauthorized access (e.g. using another's account, using a special purpose account, escalating their own privileges)
- Unauthorized monitoring (e.g. keyboard logging, network packet capturing)

3.1.11. Personal business

Computing facilities, services, and networks may not be used for compensated outside work or for unauthorized not-for-profit business activities (refer to Georgia Technology Authority Enterprise Information Security Policies, section 3.1.3, 09/10/02 and any subsequent revisions at http://gta.georgia.gov/vgn/images/portal/cit_1210/62/58/1218035EnterpriseInforSecurityPoliciesGEITLF.pdf).

3.1.12. Academic Learning Environment

Classrooms and computing facilities are provided for academic purposes. The following guidelines have been established in an effort to maintain an appropriate learning environment for students:

- No food or drinks are allowed in classrooms or computer labs.
- Users in laboratory rooms must be mindful of other people. Please maintain a quiet environment.
- Users must back up their work on their own disks. Lab computers may be moved or data on them erased at any time.
- Credit and non-credit classes always have priority in laboratories. Computer labs have scheduled hours posted on the Computer Services website and outside of the labs.

3.1.13. Duties of System Administrators

Administrators of Waycross College computing systems will perform their duties fairly, in cooperation with the user community, the higher-level administrators, University System policies, and funding sources. System administrators will respect the privacy of users as far as

possible and will refer all disciplinary matters to appropriate authorities. Student violations of these policies will be considered a violation of the student conduct code.

3.1.14. Denial of Access

Students, faculty, and staff who believe they have been unfairly denied access to computing resources at Waycross College may appeal to the Vice President and Dean or the Vice President of Business Affairs.

4. Compliance

Any person who uses Waycross College's information technology resources consents to all of the provisions of this policy and agrees to comply with all of its terms and conditions, and with all applicable federal, state, and local laws and regulations. Users have a responsibility to use these resources in an efficient, effective, ethical, and lawful manner. Violations of the policy may result in loss of usage privileges, administrative sanctions (including termination) as outlined in applicable Waycross College disciplinary procedures, as well as personal civil and/or criminal liability.

5. Policy Modifications

This policy may be changed by directive from the responsible university officer. Any changes to the policy or procedures must be promptly communicated to the individuals and offices noted in Section 6.

6. Communication

Upon approval, this policy shall be published on the Waycross College website. The following offices and individuals shall be notified via email and/or in writing upon approval of the policy and upon any subsequent revisions or amendments made to the original document:

- Vice Presidents
- Academic Division Heads
- Department Heads
- Computer Services

7. References

- Board of Regents Policy Manual
<http://www.usg.edu/regents/policymanual/>