

11.1 Campus Computer and Network Usage Policy

"Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, the right to privacy, and the right to determine the form, manner, and terms of publication and distribution. Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations, may be grounds for sanctions against members of the academic community." - The EDUCOM Code.

1. BACKGROUND AND PURPOSE

This document constitutes a College-wide policy intended to allow for the proper use of all East Georgia State College computing and network resources, effective protection of individual users, equitable access, and proper management of those resources. This should be taken in the broadest possible sense. This policy applies to East Georgia State College network usage even in situations where it would not apply to the computer(s) in use. These guidelines are intended to supplement, not replace, all existing laws, regulations, agreements, and contracts which currently apply to these services.

Academic Divisions may add, with the approval of the Division Chairperson, individual guidelines which supplement, but do not relax, this policy. In such cases, the Division should inform their users and Information Technology prior to implementation.

Access to networks and computer systems owned or operated by East Georgia State College imposes certain responsibilities and obligations and is granted subject to College policies and local, state, and federal laws. Appropriate use should always be legal, ethical, reflect academic honesty, reflect community standards, and show restraint in the consumption of shared resources. It should demonstrate respect for intellectual property; ownership of data; system security mechanisms; and individuals' rights to privacy and to freedom from intimidation, harassment, and unwarranted annoyance. Appropriate use of computing and networking resources includes instruction; independent study; independent research; communications; and official work of the offices, departments, recognized student and campus organizations, and agencies of the College.

2. DEFINITIONS

2.1. Authorized use

Authorized use of East Georgia State College-owned or operated computing and network resources is use consistent with the education, and service mission of the College, and consistent with this policy.

2.2. Authorized users

Authorized users are: (1) current faculty, staff, and students of the College; (2) anyone connecting to a public information service (see section 6.5); (3) others whose access furthers the mission of the College and whose usage does not interfere with other users' access to resources.

In addition, a user must be specifically authorized to use a particular computing or network resource by the campus department responsible for operating the resource.

3. INDIVIDUAL PRIVILEGES

It is the following individual privileges, all of which are currently existent at East Georgia State College, that empower each of us to be productive members of the campus community. It must be understood that privileges are conditioned upon acceptance of the accompanying responsibilities.

3.1. Privacy

To the greatest extent possible in a public setting we want to preserve the individual's privacy. Electronic and other technological methods must not be used to infringe upon privacy. However, users must recognize that East Georgia State College computer systems and networks are public and subject to the Georgia Open Records Act. Users, thus, utilize such systems at their own risk.

3.2. Freedom of expression

The constitutional right to freedom of speech applies to all members of the campus no matter the medium used.

3.3. Ownership of intellectual works

People creating intellectual works using East Georgia State College computers or networks, including but not limited to software, should consult Determination of Rights and Equities in Intellectual Properties (Board of Regents Policy Manual, section 6.3 and any subsequent revisions), and related East Georgia State College policies.

3.4. Freedom from harassment and undesired information

All members of the campus have the right not to be harassed by computer or network usage by others. (See section 4.1.3.)

4. INDIVIDUAL RESPONSIBILITIES

Just as certain privileges are given to each member of the campus community, each of us is held accountable for our actions as a condition of continued membership in the community. The interplay of privileges and responsibilities within each individual situation and across campus engenders the trust and intellectual freedom that form the heart of our community. This trust and freedom are grounded on each person's developing the skills necessary to be an active and contributing member of the community. These skills include an awareness and knowledge about information and the technology used to process, store, and transmit it.

4.1. Common courtesy and respect for rights of others

You are responsible to all other members of the campus community in many ways, including to respect and value the rights of privacy for all, to recognize and respect the diversity of the population and opinion in the community, to behave ethically, and to comply with all legal restrictions regarding the use of information that is the property of others.

4.1.1. Privacy of information

Files of personal information, including programs, no matter on what medium they are stored or transmitted, may be subject to the Georgia Open Records Act if stored on East Georgia State College's computers. That fact notwithstanding, no one should look at, copy, alter, or destroy anyone else's personal files without explicit permission (unless authorized or required to do so by law or regulation). Simply being able to access a file or other information does not imply permission to do so.

Similarly, no one should connect to a host on the network without advance permission in some form. People and organizations link computers to the network for numerous different reasons, and many consider unwelcome connects to be attempts to invade their privacy or compromise their security.

4.1.2. Intellectual property

You are responsible for recognizing (attributing) and honoring the intellectual property rights of others.

4.1.3. Harassment

No member of the community may, under any circumstances, use East Georgia State College's computers or networks to libel, slander, or harass any other person.

The following shall constitute Computer Harassment:

- a. Intentionally using the computer to annoy, harass, terrify, intimidate, threaten, offend or bother another person by conveying obscene language, pictures, or other materials or threats of bodily harm to the recipient or the recipient's immediate family
- b. Intentionally using the computer to contact another person repeatedly with the intent to annoy, harass, or bother, whether or not any actual message is communicated, and/or where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease
- c. Intentionally using the computer to contact another person repeatedly regarding a matter for which one does not have a legal right to communicate, once the recipient has provided reasonable notice that he or she desires such communication to cease (such as debt collection)
- d. Intentionally using the computer to disrupt or damage the academic, research, administrative, or related pursuits of another
- e. Intentionally using the computer to invade the privacy, academic or otherwise, of another or the threatened invasion of the privacy of another.

4.2. Responsible use of resources

You are responsible for knowing what information resources (including networks) are available, remembering that the members of the community share them, and refraining from all acts that waste or prevent others from using these resources or from using them in whatever ways have been proscribed by the College and the laws of the State and Federal governments. Details regarding available resources are available in many ways, including consulting with the Information Technology Department at East Georgia State College, conferring with other users, examining on-line and printed references maintained by Information Technology and others, and visiting the Student Computer Labs.

4.3. Game playing

College computing and network services are not to be used for recreational game playing. East Georgia State College reserves the right to block access to recreational game-playing web sites that may be accessed by any or all personal computers, laptops, servers, or similar computerized equipment attached to the East Georgia State College data network.

4.4. Information integrity

It is your responsibility to be aware of the potential for and possible effects of manipulating information, especially in electronic form, to understand the changeable nature of electronically stored information, and to verify the integrity and completeness of information that you compile or use. Do not depend on information or communications to be correct when they appear contrary to your expectations; verify it with the person who you believe originated the message or data.

4.5. Use of desktop systems

You are responsible in coordination with Information Technology for the security and integrity of College information stored on your personal desktop system. This responsibility includes making regular disk backups, controlling physical and network access to the machine, and installing and using virus protection software. Avoid storing passwords or other information that can be used to gain access to other campus computing resources.

4.6. Access to facilities and information

The "Rules for Use of East Georgia State College Computer Laboratories" should be followed regarding the general use of all College Computer Labs and the equipment contained in each lab. These rules are posted in each computer laboratory and are accessible on the College web page.

4.6.1. Sharing of access

Computer accounts, passwords, and other types of authorization are assigned to individual users and must not be shared with others. You are responsible for any use of your account.

4.6.2. Permitting unauthorized access

You may not run or otherwise configure software or hardware to intentionally allow access by unauthorized users. (See section 2.2.)

4.6.3. Use of privileged access

Special access to information or other special computing privileges are to be used in performance of official duties only. Information that you obtain through special privileges is to be treated as private.

4.6.4. Termination of network / account access

When a student, faculty or staff member (including instructors and participants of continuing education courses or other guests of East Georgia State College requiring network access / email accounts) is no longer an active member of East Georgia State College, the individual's network / email account access will be terminated accordingly. The following list includes but is not limited to categories and situations that warrant the termination of an EGSC network / email account:

Students: Students who have graduated from EGSC; students in non-attendance for one or more academic years. This information will be obtained and monitored via the BANNER student system.

Faculty / Staff: Termination of employment, resignation, retirement. For staff and faculty whose employment with EGSC is terminated, the respective network / email account will be terminated the same date as the employment termination date. *In order for the necessary network / email account termination process to take place on the day of termination, the college's Office of Human Resources will inform the Vice President for Information Technology concerning faculty and staff employment terminations.*

Guests of EGSC requiring temporary network / email account access: Temporary guest network / email account access will be terminated immediately upon the completion / conclusion of event(s) where an EGSC guest network / email account access was required.

For all categories, (students, faculty / staff, CE Instructors & participants, and guest users) immediate termination of network / email account access will occur in the event an individual uses an EGSC network / email account in an unauthorized manner. The sections (4.7 through 4.12) listed below include but are not limited to types of activities that could be deemed as unauthorized use of an EGSC network / email account and could lead to termination of network / email account access.

4.7. Attempts to circumvent security

Users are prohibited from attempting to circumvent or subvert any system's security measures. This section does not prohibit use of security tools by system administration personnel.

4.7.1. Decoding access control information

You are prohibited from using any computer program or device to intercept or decode passwords or similar access control information.

4.7.2. Denial of service

Deliberate attempts to degrade the performance of a computer system or network or to deprive authorized personnel of resources or access to any College computer system or network are prohibited.

4.7.3. Harmful activities

The following harmful activities are prohibited:

- a. creating or propagating viruses
- b. disrupting services
- c. damaging files
- d. intentional destruction of or damage to equipment, software, or data belonging to East Georgia State College or other users, and the like

4.7.3.1. File sharing and P2P activities

File sharing and peer-to-peer (P2P) activities are not allowed on the East Georgia State College data network.

4.7.4. Unauthorized access

You may not:

- a. damage computer systems, obtain extra resources not authorized to you, deprive another user of authorized resources, gain unauthorized access to systems, by using knowledge of:
- b. a special password, loopholes in computer security systems, another user's password, access abilities you used during a previous position at the College

4.7.5. Unauthorized monitoring

You may not use computing resources for unauthorized monitoring of electronic communications.

4.8. Academic dishonesty

You should always use computing resources in accordance with the high ethical standards of the College community. Academic dishonesty (plagiarism, cheating) is a violation of those standards.

4.9. Use of copyrighted information and materials

You are prohibited from using, inspecting, copying, and storing copyrighted computer programs and other material, in violation of copyright.

4.10. Use of licensed software

No software may be installed, copied, or used on College resources except as permitted by the owner of the software. Software subject to licensing must be properly licensed and all license provisions (installation, use, copying, number of simultaneous users, term of license, etc.) must be strictly adhered to.

4.11. Political campaigning; commercial advertising

Board of Regents policy (section 9.6.1) states "The use of USG materials, supplies, equipment, machinery, or vehicles in political campaigns is forbidden." The use of College computers and networks shall conform to these policies.

4.12. Personal business

Computing facilities, services, and networks may not be used in connection with compensated outside work nor for the benefit of organizations not related to East Georgia State College, except: in connection with scholarly pursuits (such as faculty publishing activities); or in a purely incidental way. This and any other incidental use (such as electronic communications or storing data on single-user machines) must not interfere with other users' access to resources (computer cycles, network bandwidth, disk space, printers, etc.) and must not be excessive. State law restricts the use of State facilities for personal gain or benefit.

5. EAST GEORGIA STATE COLLEGE PRIVILEGES

Our society depends on institutions like East Georgia State College to educate our citizens and advance the development of knowledge. However, in order to survive, East Georgia State College must attract and responsibly manage financial and human resources. Therefore, East Georgia State College has been granted by the State, and the various other institutions with which it deals, certain privileges regarding the information necessary to accomplish its goals and to the equipment and

physical assets used in its mission.

5.1. Allocation of resources

East Georgia State College may allocate technology resources in differential ways in order to achieve its overall mission.

5.2. Control of access to information

East Georgia State College may control access to its information and the devices on which it is stored, manipulated, and transmitted, in accordance with the laws of Georgia and the United States and the policies of the College and the Board of Regents.

5.3. Imposition of sanctions

East Georgia State College may impose sanctions and punishments on anyone who violates the policies of the College regarding computer and network usage.

5.4. System administration access

A System Administrator (i.e., the person responsible for the technical operations of a particular machine) may access others files for the maintenance of networks and computer and storage systems, such as to create backup copies of media. However, in all cases, all individuals' privileges and rights of privacy are to be preserved to the greatest extent possible.

5.5. Monitoring of usage, inspection of files

Departments of East Georgia State College operating computers and networks may routinely monitor and log usage data, such as network session connection times and end-points, CPU and disk utilization for each user, security audit trails, network loading, etc. These units may review this data for evidence of violation of law or policy, and other purposes. When necessary, these units may monitor all the activities of and inspect the files of specific users on their computers and networks. Any person who believes such monitoring or inspecting is necessary must obtain the concurrence of the Office of the Vice President for Student Affairs and Information Technology. In all cases all individuals' privileges and right of privacy are to be preserved to the greatest extent possible.

5.6. Suspension of individual privileges

Departments of East Georgia State College operating computers and networks may suspend computer and network privileges of an individual for reasons relating to his/her physical or emotional safety and well-being, or for reasons relating to the safety and well-being of other members of the campus community, or College property. Access will be promptly restored when safety and well-being can be reasonably assured, unless access is to remain suspended as a result of formal disciplinary action imposed by the Office of the Vice President for Student Affairs (for students) or the employee's department in consultation with the Vice President for Fiscal Affairs (for employees).

6. EAST GEORGIA STATE COLLEGE RESPONSIBILITIES

6.1. Security procedures

East Georgia State College has the responsibility to develop, implement, maintain, and enforce appropriate security procedures to ensure the integrity of individual and institutional information, however stored, and to impose appropriate penalties when privacy is purposefully abridged.

6.2. Anti-harassment procedures

East Georgia State College has the responsibility to develop, implement, maintain, and enforce appropriate procedures to discourage harassment by use of its computers or networks and to impose appropriate penalties when such harassment takes place.

6.3. Upholding of copyrights and license provisions

East Georgia State College has the responsibility to uphold all copyrights, laws governing access and use of information, and rules of organizations supplying information resources to members of the community (e.g., acceptable use policies for use of Internet).

6.4. Individual department responsibilities

Each department has the responsibility of:

- a. enforcing this policy
- b. providing for security in their areas
- c. providing individuals equipped with College-owned desktop systems with resources for regular disk backups (software, hardware, media, and training)

If warranted by the importance and sensitivity of information stored and processed in their facility on College-owned desktop systems, a department also has the responsibility of:

- a. performing and verifying integrity of regular media backups
- b. employing appropriate security-related software and procedures
- c. guarding confidentiality of private information, including user files and system access codes
- d. controlling physical access to equipment
- e. providing proper physical environment for equipment
- f. providing safeguards against fire, flood, theft, etc.
- g. providing proper access administration; e.g., prompt and appropriate adjustment of access permissions upon a user's termination or transfer
- h. controlling and recording software and configuration changes
- i. monitoring any system logs for access control violation attempts

East Georgia State College's Information Technology Department or appointed representative(s) serves:

as the first point of contact for unit personnel seeking problem resolution, information, and other assistance regarding computing and networking to facilitate interaction between the departments and the Office of Information and Instructional Technology at the Board of Regents.

6.5. Public information services

Department and individuals may not configure computing systems to provide information retrieval services to the public at large. (Current examples include "anonymous ftp", "Web", and "gopher.") However, centralized computing hardware and software is available for delivery of public information services, where particular attention is paid to the following sections of this policy:

2.1 (authorized use [must be consistent with College mission]), 3.3 (ownership of intellectual works), 2.1, 2.2, 4.2 (responsible use of resources), 4.9 (use of copyrighted information and materials), 4.10 (use of licensed software), and 6.4 (individual unit

responsibilities). Usage of public services will not cause computer or network loading that impairs other services.

7. PROCEDURES AND SANCTIONS

7.1. Investigative contact

If you are contacted by a representative from an external organization (District Attorney's Office, FBI, GBI, private security firm, etc.) who is conducting an investigation of an alleged violation involving East Georgia State College computing and networking resources, immediately inform the college's Vice President for Information Technology and the College's President and/or Vice President for Academic Affairs. Refer the requesting agency to the College's Vice President for Information Technology who will provide guidance regarding the appropriate actions to be taken.

7.2. Responding to security and abuse incidents

All users and departments have the responsibility to report any discovered unauthorized access attempts or other improper usage of East Georgia State College computers, networks, or other information processing equipment. If you observe, or have reported to you (other than as in 7.1 above), a security or abuse problem with any College computer or network facilities, including violations of this policy:

Take immediate steps as necessary to ensure the safety and well-being of information resources. For example, if warranted, the Information Technology Department should be contacted to temporarily disable any offending or apparently compromised computer accounts, or to temporarily disconnect or block offending computers from the network (see section 5.6).

Ensure that the following departments/people are notified: (1) Vice President for Information Technology, (2) your department head for employees (2) Office of the Vice President for Academic Affairs for students.

Reports of all incidents will be forwarded to Student Affairs (for apparent policy violations by students) or the department head (for employees), and to the Information Technology Department.

7.3. First and minor incident

If a person appears to have violated this policy, and (1) the violation is deemed minor by the Information Technology Department, and (2) the person has not been implicated in prior incidents, then the incident may be dealt with at the Information Technology Department or other department level. The alleged offender will be furnished a copy of the College Computer and Network Usage Policy (this document), and will sign a form agreeing to conform to the policy.

7.4. Subsequent and/or major violations

Reports of subsequent or major violations will be forwarded to Student Affairs (for students) or the department head (for employees) for the determination of sanctions to be imposed. Departments should consult the Office of Vice President for Fiscal Affairs/Personnel Office regarding appropriate action.

7.5. Range of disciplinary sanctions

Persons in violation of this policy are subject to the full range of sanctions, including the loss of computer or network access privileges, disciplinary action, dismissal from the College, and legal action. Some violations may constitute criminal offenses, as outlined in the Georgia Computer Systems Protection Act and other local, state, and federal laws; the College will carry out its responsibility to report such violations to the appropriate authorities.

7.6. Appeals

Appeals should be directed through the already-existing procedures established for employees and students of East Georgia State College.