## 11.4 Acceptable Use

**Overview**
Internet / Intranet / Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of East Georgia State College.

Effective security is a team effort involving the participation and support of every East Georgia State College employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

**Purpose**
The purpose of this policy is to outline the acceptable use of computer equipment belonging to East Georgia State College. These rules are in place to protect East Georgia State College, its employees, students and other users of the College's information technology. Inappropriate use exposes East Georgia State College to risks including virus attacks, compromise of network systems and services, and legal issues.

**Scope**
This policy applies to faculty, staff, students and other users (i.e., participants of East Georgia State College's Life Long Learning programs, campus visitors), contractors, consultants, temporaries, and other workers at East Georgia State College, including all personnel affiliated with third parties. This policy applies to all IT resources owned by or leased by East Georgia State College.

**Policy**

**General Use and Ownership**
1. Because of the need to protect the East Georgia State College network and IT resources/equipment, the College's Information Technology department cannot guarantee the confidentiality of information stored on any network or storage media device belonging to East Georgia State College.
2. All users (identified in Section 3.0 of this policy) are responsible for exercising good judgment regarding the reasonableness of personal use.
3. Any information users consider sensitive or vulnerable should be encrypted.
4. For security and network maintenance purposes, East Georgia State College's Information Technology Department has the right to monitor any of its IT equipment/resources, systems and network traffic at any time.
5. East Georgia State College's Information Technology Department staff reserve the right to audit / monitor / scan the college's network and/or systems and devices that connect to the college's network to ensure compliance with this policy.
6. Faculty, staff, students and other parties (e.g., participants in the College's continuing education / Life Long Learning programs) needing to connect personally owned devices to the college's network must obtain prior approval from the College's Information Technology Department.
7. All microcomputer systems connecting to the campus network must have a minimum of

10/100MB Ethernet cards installed to allow for proper connections to the College network.
8. Wiring for the campus network and any future networks installed on campus will be twisted pair category 5e (minimum requirement) cabling within the buildings and multimode fiber optic cable between buildings.
9. Only the College's Information Technology staff is authorized to provide support, perform installations of new equipment, and/or configure devices for the campus network.

**Security and Proprietary Information**

1. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
    a. Users will be required to change their respective passwords at a minimum of 90- day intervals.
2. All PCs, laptops and workstations should be secured with a password-protected Microsoft screensaver with the automatic activation feature set at 10 minutes or less, or by logging- off (use the "control-alt-delete" option Windows 2000 and XP users) when the host will be unattended.
3. Because information contained on portable computers as well as public network storage space are especially vulnerable, special care should be exercised in storing documents of a critical nature.
4. Postings by East Georgia State College faculty, staff and students with an East Georgia State College email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of East Georgia State College, unless posting is in the course of business duties.
5. All PCs, laptops, PDAs, workstations and related electronic devices used by faculty, staff and students that are connected to the East Georgia State College Internet/Intranet/Extranet, whether owned by faculty, staff or students or by East Georgia State College, shall be continually executing approved virus-scanning software with a current virus database.
6. Faculty, staff and students must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

**Unacceptable Use**

The following activities are prohibited.

Under no circumstances is an employee, student or other user of East Georgia State College's information technology infrastructure authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing East Georgia State College-owned information technology resources.

All of the items listed in the sections below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable and/or prohibited use.

**System and Network Activities**
The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by East Georgia State College.
2. Viewing pornographic or other offensive sites
3. Using campus Internet / Peachnet services for accessing / utilizing web-based game sites, including, but not limited to, web sites that include any form of gambling.
4. Engaging in electronic "pranks" such as mail bombing based on victim's sex, etc.
5. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which East Georgia State College and/or the user of East Georgia State College's information technology resources does not have an active license is strictly prohibited.
6. Downloading, copying and/or storing of copyrighted video, music files (and similar type files) via any device connected to the East Georgia State College data network
7. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The College's Information Technology Department and/or appropriate management should be consulted prior to export of any material that is in question.
8. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
9. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
10. Using an East Georgia State College IT resource to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
11. Making fraudulent offers of products, items, or services originating from any East Georgia State College network account. A network account includes accounts used by faculty, staff, students and other users of the college's information technology resources.
12. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the East Georgia State College employee, student or other user of the college's information technology infrastructure is not an intended recipient or logging into a server or account that the East Georgia State College employee, student or other user of the College's information technology infrastructure is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
13. Port scanning or security scanning is expressly prohibited.
14. Executing any form of network monitoring which will intercept data not intended for the employee, student or other college information technology user's host, unless this activity is a part of the listed individuals' normal job/duty.

15. Circumventing user authentication or security of any host, network or account.
16. Interfering with or denying service to any user other than the College's user's host (for example, denial of service attack).
17. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Peer-to-peer file-sharing software and related activities.

**Email and Communications Activities**

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
7. Users of the East Georgia State College email system must use their East Georgia State College email accounts only in support of academic pursuits and/or college business.

**Enforcement**

Any East Georgia State College employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Students of East Georgia State College found to have violated this policy may be subject to academic disciplinary action, (including being suspended from East Georgia State College for a period of time to be determined by the College's senior administration.) Other user's (e.g., participants in East Georgia State College's continuing education programs and the like) found to have violated this policy will be asked to withdraw from the specific program(s) with no reimbursement of program fees or monies paid to participate in the program(s).

Depending upon the scope of the incident, all individuals found to be in violation of this policy may be subject to penalization under local, state and/or federal laws and regulations.

**Definitions**

| Term | Definition |
|---|---|
| *Spam* | Unauthorized and/or unsolicited electronic mass mailings. |