

# GCSU

## Information Security Operational Procedures

### General Acceptable Use of Technology Resources Policy

#### INTRODUCTION

This document constitutes a university-wide policy intended to provide guidelines for the proper use of all Georgia College & State University (GCSU) computing and network resources, effective protection of individual users, equitable access, and proper management of these resources. This policy is a guide for administrators, faculty, staff, students, and official guests at GCSU in the appropriate uses of electronic and computer resources. This policy may be supplemented by other university policies. It is the user's responsibility to be aware of all relevant policy documents.

#### DEFINITIONS

**Authorized Use:** Any scholarly activity, university business activity, or personal activity by an authorized user that does not violate any Federal or state law or university policy.

**Authorized Users:** Faculty, staff currently employed by GCSU, currently enrolled students, or other individuals as approved by the Chief Information Officer (CIO) or their designee.

**Computing resources:** Refers to and includes any and all forms of computer-related equipment, tools and intellectual property. This includes computer systems, personal computers and computer networks and all forms of software, firmware, operating software and application software, owned by the university or under the university's possession, custody or control.

**E-mail:** Electronic mail.

**University Owned Computer (UOC):** Any university-owned desktop, laptop computer, or hand held computer that is assigned to or used by an authorized user.

**Personally Owned Computer (POC):** Any desktop or laptop owned by an employee or student that is used on campus or in campus housing. GCSU recognizes that principles of academic freedom, shared governance, freedom of speech, and privacy of information hold important implications for computer-mediated communication in the university environment. Personal use of campus computers in offices, computer labs, library, and other areas is allowed within reasonable limits. Authorized users shall be made aware that they are using university equipment and/or resources and such use is a reflection of the institution. Authorized users shall be aware that that they are subject to all policies while personally owned computers are connected to the university's network.

#### UNIVERSITY RIGHTS AND REMEDIES

A violation of this policy for Use of Computing Resources may subject the offender to dismissal or other sanctions after compliance with procedural due process requirements. Authorized users of the university's computing facilities are required to comply with and, by using any such facilities, agree to comply with the policies set forth by this university and the University System of Georgia (USG). The university reserves the right to amend these conditions and policies at any time without prior notice. In order to protect the integrity of GCSU's computing resources and authorized users against unauthorized or improper use of those resources the university reserves the right to:

- Limit or restrict any individual's use of; and to inspect, copy, remove or otherwise alter any data, file, or system resource that may undermine the authorized use of any computing resource.
- Disclaim responsibility for loss of data or interference with files resulting from necessary efforts to maintain the privacy and security of those computing facilities.
- Take appropriate legal action necessary to protect GCSU and its computing resources.
- Enforce the Misuse of State Property policy as stated in Georgia Department of Human Resources, Policy #1205. State property may only be used for business purposes except by exception as stated in policy #1205.

## **HARASSMENT AND THE OFFICIAL CODE OF GEORGIA**

All authorized users shall be sensitive to the public nature of shared facilities, and take care not to display images, sounds or messages that could create an atmosphere of discomfort or harassment for others. All employees and students must also refrain from transmitting to others in any location inappropriate images, sounds, or messages which might reasonably be considered harassing.

### **HARASSMENT**

Harassment, is any verbal or physical conduct, on or off campus, which has the intent or effect of unreasonably interfering with an individual's or group's educational or work performance or which creates an intimidating, hostile, or offensive educational or work environment. Harassment on the basis of race, color, gender, disability, religion, national origin, sexual orientation, or age includes harassment of an individual in terms of a stereotyped group characteristic, or because of that person's identification with a particular group. With reference to sexual harassment, the definition shall also include unwelcome sexual advances and requests for sexual favors that might be perceived as explicitly or implicitly affecting educational or employment decisions concerning an individual. It is forbidden to use e-mail or other computer communications resources to harass, offend, or annoy other users, including impeding their computing systems, software, or data. Examples of harassing computer behavior include:

- Sending unwanted and/or offensive e-mail or messages may constitute harassment and is in violation of the intended use of the system.
- Using inappropriate language. Profanity or obscenity will not be tolerated on the campus network. Each authorized user should use language appropriate for the intended recipient. Avoid offensive or inflammatory speech. Personal attacks are an unacceptable use of the network.

### **DISTRIBUTING OBSCENE MATERIAL OFFICIAL CODE OF GEORGIA -16-12-80.**

It is a violation of GCSU's policy to create, display, or transmit obscene materials, as defined in Section 16-12-80 (b) of the Official Code of Georgia, unless dissemination of the material was prohibited as provided in Section 16-12-80:

O.C.G.A. § 16-12-80

GEORGIA CODE

Copyright 2008 by The State of Georgia

All rights reserved. \*\*\* Current through the 2008 Regular Session \*\*\*

TITLE 16. CRIMES AND OFFENSES

CHAPTER 12. OFFENSES AGAINST PUBLIC HEALTH AND MORALS

ARTICLE 3. OBSCENITY AND RELATED OFFENSES

PART 1. GENERAL PROVISIONS

O.C.G.A. § 16-12-80 (2008)

§ 16-12-80. Distributing obscene material; obscene material defined; penalty

(a) A person commits the offense of distributing obscene material when he sells, lends, rents, leases, gives, advertises, publishes, exhibits, or otherwise disseminates to any person any obscene material of any description, knowing the obscene nature thereof, or offers to do so, or possesses such material with the intent to do so, provided that the word "knowing," as used in this Code section, shall be deemed to be either actual or constructive knowledge of the obscene contents of the subject matter; and a person has constructive knowledge of the obscene contents if he has knowledge of facts which would put a reasonable and prudent person on notice as to the suspect nature of the material; provided, however, that the character and reputation of the individual charged with an offense under this law, and, if a commercial dissemination of obscene material is involved, the character and reputation of the business establishment involved may be placed in evidence by the defendant on the question of intent to violate this law. Undeveloped photographs, molds, printing plates, and the like shall be deemed obscene notwithstanding that processing or other acts may be required to make the obscenity patent or to disseminate it.

(b) Material is obscene if:

(1) To the average person, applying contemporary community standards, taken as a whole, it predominantly appeals to the prurient interest, that is, a shameful or morbid interest in nudity, sex, or excretion;

(2) The material taken as a whole lacks serious literary, artistic, political, or scientific value; and

(3) The material depicts or describes, in a patently offensive way, sexual conduct specifically defined in subparagraphs (A) through (E) of this paragraph:

(A) Acts of sexual intercourse, heterosexual or homosexual, normal or perverted, actual or simulated;

(B) Acts of masturbation;

(C) Acts involving excretory functions or lewd exhibition of the genitals;

(D) Acts of bestiality or the fondling of sex organs of animals; or

(E) Sexual acts of flagellation, torture, or other violence indicating a sadomasochistic sexual relationship.

(c) Any device designed or marketed as useful primarily for the stimulation of human genital organs is obscene material under this Code section.

(d) Material not otherwise obscene may be obscene under this Code section if the distribution thereof, the offer to do so, or the possession with the intent to do so is a commercial exploitation of erotica solely for the sake of

their prurient appeal.

(e) It is an affirmative defense under this Code section that dissemination of the material was restricted to:

(1) A person associated with an institution of higher learning, either as a member of the faculty or a matriculated student, teaching or pursuing a course of study related to such material; or

(2) A person whose receipt of such material was authorized in writing by a licensed medical practitioner or psychiatrist.

(f) A person who commits the offense of distributing obscene material shall be guilty of a misdemeanor of a high and aggravated nature.

HISTORY: Ga. L. 1878-79, p. 163, § 1; Code 1882, § 4537a; Penal Code 1895, § 394; Penal Code 1910, § 385; Code 1933, § 26-6301; Ga. L. 1935, p. 158, § 1; Ga. L. 1941, p. 358, § 1; Ga. L. 1956, p. 801, § 1; Ga. L. 1963, p. 78, § 1; Code 1933, § 26-2101, enacted by Ga. L. 1968, p. 1249, § 1; Ga. L. 1971, p. 344, § 1; Ga. L. 1975, p. 498, §§ 1, 2; Ga. L. 1992, p. 6, § 16; Ga. L. 1996, p. 6, § 16.

## **ELECTRONIC MAIL USE**

Complete details concerning email policies are found in the Electronic Communications Policy.

## **PRIVACY & SECURITY**

E-mail is an academic asset and critical component of the GCSU's communication procedures. Official GCSU e-mail systems are provided to help employees and students in the performance of their duties or studies. GCSU attempts to afford e-mail privacy protections comparable to that which it traditionally affords paper, mail, and telephone communications. GCSU and system administrators do not routinely inspect, monitor, or disclose e-mail content. Neither can the university, in general, protect users from receiving e-mail they may find offensive. Employees and students of GCSU, however, are strongly encouraged to use the same personal and professional courtesies and considerations in e-mail as they would in other forms of communication. Network and computer operations personnel need, from time to time, to observe certain transactional addressing information to ensure proper functioning of GCSU's e-mail services. On these and other occasions, the content of e-mail may be inadvertently read. Except as provided elsewhere in this policy, they are not permitted to see or read the contents intentionally; to read transactional information where not germane to the foregoing purpose; or disclose or otherwise use what they have seen. One exception, however, is that of systems personnel (such as "postmasters") who may need to inspect e-mail when rerouting or disposing of otherwise undeliverable e-mail. This exception is limited to the least invasive level of inspection required to perform such duties. Authorized users should consider their use of the university e-mail and how it reflects on GCSU's image as all e-mail; both personal and business, may be subject to public disclosure. Authorized users are forewarned of the following:

- E-mail, whether or not created or stored on university equipment, may constitute a university record and is subject to disclosure under the Georgia Open Records Act, other laws, or as a result of litigation.

- The confidentiality of e-mail cannot be assured and may be compromised by applicability of law or policy, including this policy, by unintended redistribution, or because of the inadequacy of current technologies to protect against unauthorized access.
- E-mail distribution of confidential personal information or other confidential information (confidential student records, for example) is prohibited.  
GCSU has no control over the security of e-mail that has been downloaded to an authorized user's computer. As a deterrent to potential intruders and to misuse of e-mail, authorized users should employ whatever protections (such as passwords and encryptions) are available to them.

### **Employee Responsibilities Related to the Use of E-mail**

Authorized users of GCSU's e-mail systems shall not:

- Subscribe to multiple high volume listservs, newsletters, etc. that would place a burden on the system.
- Intentionally cause disruption, damage, or excessive strain on any computing resources, or unwarranted or unsolicited interference with others' use of e-mail or e-mail systems.
- Create or willfully disseminate computer viruses. Each employee and student should be sensitive to the ease of spreading viruses and should take steps to insure files are virus free.
- Give out an authorized user's e-mail password to anyone.
- Fail to follow policies appropriate to mail list usage.
- Solicit to buy or sell goods or services for personal profit, except as permitted on designated lists.
- Manage storage of email on the server so as to best utilize server storage space.
- Display or transmit sexually explicit images, messages, or cartoons.

### **UNIVERSITY RESPONSIBILITIES RELATED TO THE USE OF E-MAIL**

University Information Technology (IT) staff will maintain system level security of mail servers. They will remain aware of security warnings pertaining to server software and take appropriate action.

IT staff will not allow access of user e-mail by anyone other than the mail server administrator and the account holder. The server administrator will only examine user mail when necessary, as provided by this policy (i.e. for the recovery of lost mail or system failure).

### **USER RESPONSIBILITIES RELATED TO NETWORK USE**

Employees and students of GCSU may use the university's computing resources including transmission over the university network, for scholarly purposes, for official university business, and for personal purposes so long as such use does not:

- Violate any Federal or state law or university policy,
- Involve significant use of university resources or direct costs,
- Substantially interfere with the performance of university duties, work, or data communications networks, and/or
- Conflict with the State policy on Misuse of State Property.

Authorized users of GCSU's network resources shall not:

- Create or willfully disseminate computer viruses. Authorized users shall be sensitive to the ease of spreading viruses and shall take steps to insure computer files are virus free.
- Allow non-authorized users access to passwords or share accounts. It is the authorized user's responsibility to protect any account from unauthorized use by following security procedures.
- Attempt to circumvent system security, guess other passwords, or in any way gain unauthorized access to local or network resources. Users may not use another person's computing account, attempt to forge an account, or use a false account or e-mail address.
- Transfer copyrighted materials to or from any system or via the university network without express consent of the owner as this may be a violation of Federal and/or State Law.

## **COMPUTER LABS AND ELECTRONIC CLASSROOMS**

Authorized users in campus computer labs shall follow these additional guidelines:

- Show current GCSU identification (Bobcat card) or Faculty/Staff ID upon entering the computer lab. All users must sign in on entry or swipe their identification card as available.
- Reconfigure computers, changing colors or fonts, installing/uninstalling software, moving equipment or in any way trying to change the set up of the computers.
- Keep noise levels to a minimum.

All authorized users shall avoid the following:

- Connecting to other computers without explicit permission.
- Bringing children, food or drinks into the computer labs.
- Attempting to circumvent security mechanisms.
- Attempting to intercept or decode passwords or similar information.
- Attempting to deliberately degrade performance, deny service, or disrupt services.
- Using the lab phone for personal calls.
- Accessing anyone else's account(s).

- Attempting to damage files, equipment, software, or data.
- Using formerly privileged access after graduation, transfer, or termination.
- Using computer lab resources for political campaigns or commercial advertising.

## **HELP DESK (SERVE)**

The SERVE help desk is the official location designed to receive all technology questions regarding PAWS, CATS, or other Banner related services; as well as computers, network, audio / visual needs, and television. The SERVE representatives will attempt, through a series of questions, to resolve the problem by phone. If the representative is unable to resolve the problem, a service request will be placed. A support technician will respond to all requests as soon as possible.

## **VII. Software**

GCSU provides many software programs and data obtained under contracts or licenses and distributes them across campus. These resources may not be copied, altered, or distributed without consent of the Chief Information Officer (CIO) or their designee. GCSU offices and departments requiring special software should discuss it prior to purchase/acquisition with the CIO or their designee to ensure that it is compatible, nonduplicative and will work within the existing GCSU infrastructure. IT will place the order for the software charging back costs as appropriate. The license and original copy of the media will be held by IT. Any software installed on an UOC must be a legal copy, approved and installed by IT.