

Appendix Q

Computer and Network Usage Policy

1. Background and Purpose

This document constitutes a campus-wide policy intended to allow for the proper use of all Georgia Southwestern State University computing and network resources, effective protection of individual users, equitable access to, and proper management of those resources. This policy applies to Georgia Southwestern State University 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. The different computer labs located throughout campus may post additional operational rules and restrictions that are considered part of this policy. Users are responsible for reading and following these rules. Access to networks and computer systems owned or operated by Georgia Southwestern State University imposes certain responsibilities and obligations and is granted subject to university 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; authorized research; independent research; communications; and official work of the offices, units, recognized student and campus organizations, and agencies of the university.

2. Definitions

2.1 Campus Technology Services

Support for computing functions on the Georgia Southwestern State University campus is the responsibility of Information and Instructional Technology (IIT).

2.2 Authorized users

Individuals who have been granted and hold an active and authorized account on a GSW computer or network and abide by this policy are considered authorized users.

2.3 Authorized use

Authorized use is predicated on access by an authorized user. Authorized use is usage that is consistent with the academic, research and service goals of this institution and that falls within the guidelines of this policy and the policy of the Board of Regents which states that property owned by the institution shall be used only for institutional purposes. Any individually owned computer or electronic device connected to the campus network is also subject to the guidelines of this policy. Placement of any network device such as servers, modems, hubs, routers, switches, cameras, etc., must be approved by IIT prior to being connected to the network. Residence Hall occupants may connect one computer to the campus network for personal use only.

3. Individual privileges

The following individual user privileges are granted contingent upon acceptance of the accompanying individual responsibilities (see 4.) These privileges are based on each person developing the skills necessary to be a competent user of computing resources.

3.1 Privacy

To the greatest extent possible in a public setting the university wants to preserve the individual's privacy. The Information Technology professionals at GSW are committed to preserving the privacy of each authorized user of the computer systems. However, it is impossible to guarantee such privacy and users must be aware of several specific issues. Electronic mail messages are not secure and therefore should not be assumed to be private. Also, despite best efforts to prevent it, a determined person could gain unauthorized access to stored data and thus violate your privacy. Under the Georgia Open Records law it is possible that information stored on a computer system, including electronic mail, would be available for inspection by any member of the public. Finally, in the process of performing normal system/network management and auditing functions, it may be necessary to view user's files or confidential information. However, system, network and application administrators are bound by both professional ethics as well as job requirements to respect the privacy of those involved and not initiate disclosure of information obtained in this manner unless it is discovered that provisions of this policy or existing state or federal laws have been violated. Users shall not perform security scanning, probing or monitoring services without appropriate permission.

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 Georgia Southwestern State University computers or networks, including but not limited to software, should consult Determination of Rights and Equities in Intellectual Property (Board of Regents Policy Manual, section 603.03, 2/2/94 and any subsequent revisions).

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 4.1.3).

4. Individual responsibilities

Individual users are expected to accept the responsibilities outlined in this section.

4.1 Common courtesy and respect for rights of others

Individual users are responsible to all other members of the campus community in many ways, including to respect and value the rights of privacy for all, 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 software programs, no matter on what medium they are stored or transmitted, are subject to the Georgia Open Records Act (<http://www.sos.state.ga.us/Archives/rms/ora.htm>) if stored on Georgia Southwestern State University's computers (see section 5.2). 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 connections to be attempts to invade their privacy or compromise their security.

4.1.2 Intellectual property

Individual users are responsible for honoring the intellectual property rights of others.

4.1.3 Harassment

No member of the community may, under any circumstances, use Georgia Southwestern State University's computers or networks to libel, slander, or harass any other person. The following shall constitute computer harassment:

- (1) 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.
- (2) 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;
- (3) 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);
- (4) Intentionally using the computer to disrupt or damage the academic, research, administrative, or related pursuits of another;
- (5) 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

Individual users are responsible for knowing what information resources are available, remembering that the members of the University 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 University and the laws of the state and federal governments. Programs that use large amounts of bandwidth may be disabled if they interfere with academic or administrative functions.

4.3 Recreational activities

Recreational use of Georgia Southwestern State University computing resources is prohibited to the extent this activity interferes with academic pursuits. Recreational computing includes game playing and downloading music or video files.

4.4 Information integrity

It is the user's 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 is compiled or used.

4.5 Desktop systems integrity

Users may not install hardware or change equipment configurations on desktop PC systems without prior approval of Information and Instructional Technology. Users may not install software on desktop PC systems located in public computing facilities. Installation of software on assigned desktop systems will be subject to provisions outlined in section 4.11.

4.6 Use of desktop systems - Users are responsible for the security and integrity of University information stored on assigned desktop systems. This responsibility includes making regular backups, and controlling physical and network access to the machine. Users must protect passwords or other information that can be used to gain access to other campus computing resources.

4.7 Access to facilities and information

4.7.1 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.

4.7.2 Permitting unauthorized access

Users may not run or otherwise configure software or hardware to intentionally allow access by unauthorized users (see section 2.3).

4.7.3 Use of privileged access

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

4.7.4 Termination of access

When a user ceases being a member of the campus community (graduates or terminates employment), or is assigned a new position and/or responsibilities within the University, access authorization may be reviewed. Users must not use facilities, accounts, access codes, privileges, or information not authorized in the new circumstances.

4.8 Attempts to circumvent security

4.8.1 Decoding access control information

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

4.8.2 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 University computer system or network are prohibited.

4.8.3 Harmful activities

The following harmful activities are prohibited: creating or propagating viruses; disrupting services, damaging files, intentional destruction of or damage to equipment, software, or data belonging to Georgia Southwestern State University or other users; and the like.

4.8.4 Unauthorized access

Individual users may not damage computer systems, obtain extra resources not previously authorized, deprive another user of authorized resources, access abilities used during a previous position at the University, or gain unauthorized access to systems by using knowledge of a special password, loopholes in computer security systems, or another user's password.

4.8.5 Unauthorized monitoring

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

4.9 Academic dishonesty

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

4.10 Use of copyrighted information and materials

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

4.11 Use of licensed software

No software may be installed, copied, or used on university resources except as permitted by the publisher 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. All software installed on campus computers must be approved by Information and Instructional Technology.

4.12 Political campaigning/commercial advertising

The Board of Regents policy (section 914.01) states, "The use of System materials, supplies, equipment, machinery, or vehicles in political campaigns is forbidden." The use of university computers and networks shall conform to this policy.

4.13 Personal business

Computing facilities, services, and networks may not be used in connection with compensated outside work or for the benefit of organizations not related to Georgia Southwestern State University, except in connection with traditional faculty pursuits such as teaching, research, and service. 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 (network bandwidth, disk space, printers, etc.) and must not be excessive. State law restricts the use of state facilities for personal gain or benefit.

4.14 State of Georgia Policy on Pornographic Material

According to State of Georgia policy of the Appropriate Use of Information Technology Resources (Policy Number 3.1.3) creation, accessing or transmitting sexually explicit, obscene or pornographic material is prohibited.

5. Georgia Southwestern State University Privileges

Georgia Southwestern State University retains certain privileges regarding the information necessary to manage the equipment and physical assets used in accomplishing its mission.

5.1 Allocation of resources

Georgia Southwestern State University allocates resources in order to achieve its overall mission.

5.2 Control of access to information

Georgia Southwestern State University 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 university and the Board of Regents. Georgia Southwestern State University reserves the right to remove data and/or program files from the network file servers and computers located in classrooms and labs and from other publicly accessible equipment.

5.3 Imposition of sanctions

Georgia Southwestern State University may impose sanctions and punishments on anyone who violates the policies of the university regarding computer and network usage.

5.4 System administration access

Electronic mail, information passing over the university network, and information stored in user accounts are generally considered to be private and confidential. Although this type of information must be accessed by system personnel for the purpose of backups, network management, etc., the content of user files and network transmissions will not be viewed, monitored, or altered without the express permission of the user except in the following circumstances:

- the university has reason to believe that an account or system has been breached and is being used by someone other than the authorized user;
- the university has received a complaint that an account or system is being used to gain unauthorized access or to attempt to gain unauthorized access to another network site; or
- the university has reason to believe that an account is being used in violation of university policies, federal, or state law.

Under these circumstances, the Director of IIT, or his/her designee, may authorize system support personnel to monitor the activities of a specified account or computer system and to search electronic information stored in that account. However, in all cases, individuals' privileges and rights of privacy are to be preserved to the greatest extent possible.

5.5 Monitoring of usage, inspection of files

Georgia Southwestern State University 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. In all cases, an individual's privileges and right of privacy are to be preserved to the greatest extent possible. If during the process of the routine activities, IIT discovers a clear violation of policy (e.g. pornographic material) this violation will be reported to Office of the Dean of Students (for students) or HR director (for employees).

5.6 Suspension of individual privileges

Georgia Southwestern State University may suspend computer and network privileges of an individual as a result of formal disciplinary action imposed by the Office of the Dean of Students (for students) or the employee's department in consultation with the appropriate administrator.

5.7 Suspension of a network connection

IIT will temporarily disconnect a suspect computer from the network if the situation warrants. A computer could be temporarily disconnected from the network as a result of evidence of excessive bandwidth use from obvious peer to peer traffic or if there is evidence a computer has a virus or evidence that a computer has been hacked and is being used to illegally share files. A computer may also be temporarily disconnected from the network as the result of an abuse report filed at USG IIT Customer Services Abuse

abuse@usg.edu or with GSW IIT Abuse (<http://www.gsw.edu/~oiit/abuse.shtml>) or abuse@gsw.edu.

6. Georgia Southwestern State University Responsibilities

6.1 Security procedures

Georgia Southwestern State University 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

Georgia Southwestern State University 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. The Georgia Southwestern State University harassment policies can be found at <http://www.gsw.edu/~hr/publications/POLICY.htm>.

6.3 Upholding of copyrights and license provisions

Georgia Southwestern State University 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 Unit responsibilities

Each unit has responsibility for:

- enforcing this policy
- protecting confidentiality of private information, including user files and system access codes (passwords)
- controlling physical access to equipment
- providing proper physical environment for equipment
- utilizing institutional safeguards against fire, flood, theft, etc.
- giving prompt notification to IIT of the user's termination or transfer

7. Procedures and Sanctions

7.1 Investigative contact

If a user is contacted by a representative from an external organization (District Attorney's office, FBI, GBI, Southern Bell Security Services, etc.) who is conducting an investigation of an alleged violation involving Georgia Southwestern State University computing and networking resources, the user must inform IIT and the Vice President for Business and Finance (VPBF) immediately. The VPBF together with the Director of IIT will provide guidance regarding the appropriate actions to be taken.

7.2 Responding to security and abuse incidents / Computer Incident Response Team - CIRT

All users and units have the responsibility to report any discovered unauthorized access attempts or other improper usage of Georgia Southwestern State University computers, networks, or other information processing equipment. If a user observes or has reported (other than as in 7.1 above) a security or abuse problem with any university computer or network facility, including violations of this policy, the user should contact IIT immediately at 931-2074, abuse@gsw.edu or <http://www.gsw.edu/~oiit/abuse.shtml>.

7.3 First and minor incident

If a person appears to have violated this policy, and (1) the violation is deemed minor, and (2) the person has not been implicated in prior incidents, then the incident may be dealt with by the IIT CIRT team. If warranted, the violation will be reported to the Vice President for Student Affairs (for students), the HR Director (for all others) and the Director of Information and Instructional Technology. The alleged offender will be furnished a copy of the university Computer and Network Usage Policy (this document).

7.4 Subsequent and/or major violations

Reports of subsequent or major violations will be forwarded to the Vice President for Student Affairs (for students), the HR Director and Vice President for Academic Affairs (for all others), and the Director of IIT for the determination of sanctions to be imposed. Copies of the imposed sanctions will be sent to the Vice President for Academic Affairs, the Vice President for Business and Finance, and the Director of IIT. Unit Heads should consult the appropriate Vice President regarding appropriate action to be taken.

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 university, 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 university 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.