

*This portion of the document has been copied from the OIT web page for your information.  
For the latest information, see <http://www.oit.gatech.edu/oithome/policy.html>*

*Georgia Institute of Technology  
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 an Institute-wide policy intended to allow for the proper use of all Georgia Tech 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 Georgia Tech network usage even in situations where it would not apply to the computer(s) in use. These guidelines are intended to supplement, not to replace, all existing laws, regulations, agreements, and contracts that currently apply to these services.*

*Campus units that operate their own computers or networks may add, with the approval of the unit head, individual guidelines which supplement, but do not relax, this policy. In such cases, the unit should inform their users and the Information Resources Security Coordinator in OIT prior to implementation.*

*Access to networks and computer systems owned or operated by Georgia Tech imposes certain responsibilities and obligations and is granted subject to Institute 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 Institute.*

## 2. DEFINITIONS

### 2.1. Authorized use

*Authorized use of Georgia Tech-owned or operated computing and network resources is use consistent with the education, research, and service mission of the Institute, and consistent with this policy.*

### 2.2. Authorized users

*Authorized users are: (1) current faculty, staff, and students of the Institute; (2) anyone connecting to a public information service (see section 6.5); (3) others whose access furthers the mission of the Institute and whose usage does not interfere with other users' access to resources. The policy Access by External Entities to Institute Information Technology Resources (OIT, 11/3/93, and any subsequent revisions) may apply. In addition, a user must be specifically authorized to use a particular computing or network resource by the campus unit responsible for operating the resource.*

## 3. INDIVIDUAL PRIVILEGES

*It is the following individual privileges, all of which are currently existent at Georgia Tech, 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 Georgia Tech 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 Georgia Tech 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), and related Georgia Tech 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 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 Georgia Tech'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 Georgia Tech'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*

*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 Institute and the laws of the State and Federal governments. Details regarding available resources are available in many ways, including consulting your Computing Support Representative (CSR) (see section 6.4), conferring with other users, examining on-line and printed references maintained by OIT and others, visiting the OIT Information Center, and contacting the OIT Helpdesk.*

#### *4.3. Game playing*

*Limited recreational game playing, that is not part of an authorized and assigned research or instructional activity, is tolerated (within the parameters of each department's rules). Institute computing and network services are not to be used for extensive or competitive recreational game playing. Recreational game players occupying a seat in a public computing facility must give up that seat when others who need to use the facility for academic or research purposes are waiting.*

#### *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 your CSR for the security and integrity of Institute 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*

##### 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 access*

*When you cease being a member of the campus community (graduate or terminate employment), or if you are assigned a new position and/or responsibilities within the Institute, your access authorization must be reviewed. You must not use facilities, accounts, access codes, privileges, or information for which you are not authorized in your new circumstances.*

#### 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 Institute computer system or network are prohibited.*

#### 4.7.3. 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 Tech or other users; and the like.*

#### 4.7.4. Unauthorized access

*You may not:*

- \* 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:*

- \* a special password*
- \* loopholes in computer security systems*
- \* another user's password*
- \* access abilities you used during a previous position at the Institute*

#### 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 Institute 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 Institute 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 914.01) states "The use of System materials, supplies, equipment, machinery, or vehicles in political campaigns is forbidden." The Georgia Tech Faculty Handbook (section 6.15.3.8(b)) states "Political campaign and commercial advertisement shall not be displayed on the campus." The use of Institute 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 Georgia Tech, except: in connection with scholarly pursuits (such as faculty publishing activities); in accordance with the Institute Consulting Policy or the policy Access by External Entities to Institute Information Technology Resources (OIT, 11/3/93, and any subsequent revisions); 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. GEORGIA TECH PRIVILEGES*

*Our society depends on institutions like Georgia Tech to educate our citizens and advance the development of knowledge. However, in order to survive, Georgia Tech must attract and responsibly manage financial and human resources. Therefore, Tech 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*

*Georgia Tech may allocate resources in differential ways in order to achieve its overall mission.*

#### *5.2. Control of access to information*

*Georgia Tech 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 Institute and the Board of Regents.*

### 5.3. *Imposition of sanctions*

*Georgia Tech may impose sanctions and punishments on anyone who violates the policies of the Institute 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*

*Units of Georgia Tech 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 unit head and the campus Legal Division. 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*

*Units of Georgia Tech 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 Institute 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 Services (for students) or the employee's department in consultation with the Office of Human Resources (for employees).*

## 6. *GEORGIA TECH RESPONSIBILITIES*

### 6.1. *Security procedures*

*Georgia Tech 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 Tech 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*

*Georgia Tech 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 unit responsibilities*

*Each unit has the responsibility of:*

- \* enforcing this policy*
- \* providing for security in their areas*
- \* providing individuals equipped with Institute-owned desktop systems with resources for regular disk backups (software, hardware, media, and training) and for virus protection*

*If warranted by the importance and sensitivity of information stored and processed in their facility, a unit must also:*

- \* provide system administration personnel*
- \* perform and verify integrity of regular media backups*
- \* employ appropriate security-related software and procedures*
- \* guard confidentiality of private information, including user files and system access codes*
- \* control physical access to equipment*
- \* provide proper physical environment for equipment*
- \* provide safeguards against fire, flood, theft, etc.*
- \* provide proper access administration; e.g., prompt and appropriate adjustment of access permissions upon a user's termination or transfer*
- \* control and record system software and configuration changes*
- \* monitor system logs for access control violation attempts*

*Units are to designate a person employed by the unit as their Computing Support Representative (CSR); the Director of Client Services, Office of Information Technology is to be notified of CSR appointments. CSRs should be knowledgeable about their unit's computing environment and about central resources and services. The CSR 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 unit and the Office of Information Technology*

## 6.5. *Public information services*

*Units and individuals may, with the permission of the appropriate unit head, configure computing systems to provide information retrieval services to the public at large. (Current examples include "anonymous ftp" and "gopher.") However, in so doing, particular attention must be paid to the following sections of this policy: 2.1 (authorized use [must be consistent with Institute mission]), 3.3 (ownership of intellectual works), 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 must 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, Southern Bell Security Services, etc.) who is conducting an investigation of an alleged violation involving Georgia Tech computing and networking resources, inform the office of the Executive Director for Information Technology (EDIT) and the Chief Legal Advisor immediately. Refer the requesting agency to the EDIT office; that office will provide guidance regarding the appropriate actions to be taken.*

### 7.2. *Responding to security and abuse incidents*

*All users and units have the responsibility to report any discovered unauthorized access attempts or other improper usage of Georgia Tech 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 Institute 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, a system administrator 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 people are notified: (1) your Computing Support Representative, (2) your unit head, (3) the Information Resources Security Coordinator (IRSC), who is located within the Office of Information Technology.*

*The IRSC will coordinate the technical and administrative response to such incidents. Reports of all incidents will be forwarded to Student Services (for apparent policy violations by students) or the unit head (for employees), and to the Executive Director for Information Technology and the Chief Information Officer.*

### *7.3. First and minor incident*

*If a person appears to have violated this policy, and (1) the violation is deemed minor by OIT, and (2) the person has not been implicated in prior incidents, then the incident may be dealt with at the OIT or unit level. The alleged offender will be furnished a copy of the Institute 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 Services (for students) or the unit head (for employees) for the determination of sanctions to be imposed. Units should consult the Office of Human Resources 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 Institute, 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 Institute 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.*

*Rev. 8/94*