

Georgia Institute of Technology

COMPUTER AND NETWORK USAGE POLICY

June 6, 2001

“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, 1987

<http://www.educause.edu/>

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 document should be broadly interpreted. 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 replace, all existing laws, regulations, agreements, and contracts that currently apply to computing and networking services.

Campus units that operate their own computers or networks are encouraged to add, with the approval of the unit head, individual guidelines that supplement, but do not lessen the intent of this policy. In such cases, the unit will inform users and provide a

copy of the unit-level policy to the Office of Information Technology, Information Security Directorate upon implementation.

Access to the Georgia Tech Network is a privilege, not a right. Access to networks and computer systems owned or operated by Georgia Tech requires certain user responsibilities and obligations and is subject to Institute policies and local, state, and federal laws. Appropriate use should always be legal and ethical. Users should reflect academic honesty, mirror community standards, and show consideration and restraint in the consumption of shared resources. Users should also demonstrate respect for intellectual property; ownership of data; system security mechanisms; and individual rights to privacy and to freedom from intimidation, harassment, and annoyance. Appropriate use of computing and networking resources includes instruction; independent study; authorized research; independent research; communications; and official work of GT 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) individuals connecting to a public information service (see section 6.5); and (3) others whose access furthers the mission of the Institute and whose usage does not interfere with other authorized users' access to resources. The policy Access by External Entities to Institute Information Technology (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

The following individual privileges, all of which currently exist at Georgia Tech, empower all members of the Georgia Tech community to be productive members of that community. It must be understood that privileges are conditioned upon acceptance of the accompanying responsibilities within the guidelines of the Computer and Network Usage Policy.

3.1. Privacy

To the greatest extent possible in a public setting, Georgia Tech seeks to preserve individual privacy. Electronic and other technological methods must not be used to infringe upon privacy. However, Georgia Tech computer systems and networks are public and subject to the Georgia Open Records Act. All content residing on Institute systems is subject to inspection by the Institute.

For information on monitoring network usage and file inspections, please reference section 5.5.

3.1.1. Encryption and password protection

Encryption utilities or password protection schemes requiring data recovery via a password or encryption key may not be used on the Institute's systems without unit-level approval of a recovery process.

3.2. Ownership of intellectual works

Anyone 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 (refer to Board of Regents Policy Manual, section 603.03, 2/2/94 and any subsequent revisions at <http://www.usg.edu/admin/policy/600.phtml> and related Georgia Tech policies).

3.3. Freedom from harassment and undesired information

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

4. INDIVIDUAL RESPONSIBILITIES

Just as each member of the campus community enjoys certain privileges, so too is each member of the community responsible for his or her actions. The interplay of these privileges and responsibilities engenders the trust and intellectual freedom that form the heart of this community. The trust and freedom that exists are grounded in each person's developing the skills necessary to be an active and contributing member of the community. These skills include 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

Users are responsible to all other members of the campus community in many ways. They include the responsibility to:

- Respect and value the right of privacy,
- Recognize and respect the diversity of the population and opinion in the community, and
- Comply with Institute policy and all laws and contracts regarding the use of information that is the property of others.

4.1.1. Privacy of information

Files of personal information, including programs, but regardless of storage medium or transmittal, are subject to the Georgia Open Records Act if stored on Georgia Tech's computers (see section 3.1). Nonetheless, individuals are prohibited from looking at, copying, altering, or destroying anyone else's personal files without explicit permission (unless authorized or required to do so by law or regulation). The ability to access a file or other information does not imply permission to do so.

4.1.2. Intellectual property

Users are responsible for recognizing 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 harass any other person.

The following constitutes 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 an actual message is communicated, and/or the 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; and (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

Users 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 online and printed references maintained by OIT and others, and visiting the OIT Customer Support Center or its website at <http://www.oit.gatech.edu/cs>

4.2.1. Domain Names

Requests to establish new domain names within the Georgia Tech network domain will be forwarded to the Office of Information Technology. Requests for names not ending in “gatech.edu” will not normally be approved. All such requests require the approval of the Associate Vice President and Associate Vice Provost for Information Technology.

4.3. Information Integrity

Each individual is responsible for being aware of the potential for and possible effects of manipulating information, especially in electronic form. Each individual is responsible for understanding the changeable nature of electronically stored information, and to verify the integrity and completeness of information compiled or used. No one should depend on information or communications to be correct when they appear contrary to expectations. It is important to verify that information with the source.

4.4. Use of personally managed systems

Personally managed systems are not limited to computers physically located on the campus, but include any type of device that can be used to access Institute computing and networking resources from any location.

Authorized users have a responsibility to ensure the security and integrity of system(s) accessing other computing and network resources of the Institute, whether you are a student, employee, or other authorized user. Institute information electronically stored therein must be protected.

Appropriate precautions for personally owned or managed systems include performing regular backups, controlling physical and network access, using virus protection software, and keeping any software installed (especially anti-virus and operating system software) up to date with respect to security patches.

http://www.security.gatech.edu/system_admin.html

Authorized users must ensure compliance with the security, software, and support policies of their unit. The CSR of the unit is an appropriate resource to consult with regarding these policies.

4.5. Access to facilities and information

4.5.1. 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.

4.5.2. Permitting unauthorized access

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

4.5.3. Use of privileged access

Access to information should be provided within the context of an authorized user's official capacity with the Institute. Authorized users have a responsibility to ensure the appropriate level of protection over that information.

4.5.4. Termination of access

When an authorized user changes status (e.g., terminates employment, graduates, retires, changes positions or responsibilities within the Institute, etc.), the unit responsible for initiating that change in status must coordinate with the user to ensure that access authorization to all Institute resources is appropriate. An individual may not use facilities, accounts, access codes, privileges, or information for which he/she is not authorized.

4.6. 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 personnel authorized by OIT or their unit.

4.6.1. Decoding access control information

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

4.6.2. 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.

4.6.3. Harmful activities

Harmful activities are prohibited. Examples include IP spoofing; creating and propagating viruses; port scanning; disrupting services; damaging files; or intentional destruction of or damage to equipment, software, or data.

4.6.4. Unauthorized access

Authorized users may not:

- *Damage computer systems
- *Obtain extra resources not authorized to them
- *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 used during a previous position at the Institute

4.6.5. Unauthorized monitoring

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

4.7. Academic dishonesty

Authorized users should always use computing resources in accordance with the high ethical standards of the Institute community. Academic dishonesty is a violation

of those standards, including the Academic Honor Code.

<http://www.honor.gatech.edu>

4.8. Use of copyrighted information and materials

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

4.9. 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.

4.10. Political campaigning; commercial advertising

Please refer to Board of Regents Policy (Section 914.01)

<http://www.usg.edu/admin/policy/900.phtml>

4.11. 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 accordance with the Institute Consulting Policy or the policy Access by External Entities to Institute Information Technology Resources. State law restricts the use of state facilities for personal gain or benefit.

5. GEORGIA TECH PRIVILEGES

Our society depends on institutions such as 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 protect 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

Users should also be aware that their uses of Georgia Tech's computing resources are not completely private. While the Institute does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of the

Institute's computing resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for maintaining network availability and performance.

The Institute may also specifically monitor the activity and accounts of individual users of the Institute's computing resources, including individual login sessions and communications, without notice. This monitoring may occur in the following instances:

1. The user has voluntarily made them accessible to the public.
2. It reasonably appears necessary to do so to protect the integrity, security, or functionality of the Institute or to protect the Institute from liability.
3. There is reasonable cause to believe that the user has violated, or is violating, this policy.
4. An account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns.
5. Upon receipt of a legally served directive of appropriate law enforcement agencies.

Any such individual monitoring, other than that specified in "(1)", required by law, or necessary to respond to bona fide emergency situations, must be authorized in advance by the Chief Legal Advisor or his/her designee and the Associate Vice President and Associate Vice Provost for Information Technology; in all such cases, the appropriate unit head will be informed as time and the situation will allow. In all cases, all individuals' privileges and right of privacy are to be preserved to the greatest extent possible.

For further information, please see 3.1 for information on privacy.

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 Affairs (for students) or the employee's department in consultation with the Office of Human Resources (for employees).

6. GEORGIA TECH RESPONSIBILITIES

6.1. Risk management

Georgia Tech, through the Department of Internal Auditing, maintains a periodic risk evaluation process to protect its information systems infrastructure and data in the face of a changing information security environment. All unit heads are required to approve an annual risk evaluation conducted by the unit with a semi-annual follow-up on identified risks.

Benefits of a properly performed risk analysis include:

- Increase security awareness at all organizational levels from operations to management.
- Evaluate the status of the current security posture.
- Highlight areas where greater security is needed.
- Assemble facts, dispel myths, and fight complacency.
- Justify, prioritize, and implement effective counter-measures and procedures.

These evaluations will entail a thorough review of each unit's information security policy, procedures, and practices.

The aggregate of Unit Information Systems Risk Evaluations will be based on results from the Unit Risk Evaluations collected by the OIT Information Security Directorate and assembled with collaboration from Internal Auditing. The results and recommendations will be submitted to the President's Office semi-annually.

Units will develop a policy for purchasing computing resources to ensure these resources fit the unit's technology architecture and are properly supported.

6.2. 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, and to impose appropriate penalties when privacy is purposefully abridged.

6.3. Anti-harassment procedures

Georgia Tech has the responsibility to develop, implement, maintain, and enforce appropriate procedures to discourage harassment through the use of its computers or networks and to impose appropriate penalties when such harassment takes place. Georgia Tech's anti-harassment policy and procedures are available at: <http://www.admin-fin.gatech.edu/human/relations/070500.html>

6.4. Upholding of copyrights and license provisions

Georgia Tech has the responsibility to uphold all copyrights, laws governing access and use of information, and rules or contractual requirements of organizations supplying information resources to members of the community (e.g., Internet acceptable use policies and license requirements for commercial information databases). The Georgia Tech Library maintains copies of relevant copyright laws and guidelines at: http://www.library.gatech.edu/resvcopyright_frame.htm

6.5. Individual unit responsibilities

Each unit is responsible for compliance with Section 6. Units are to designate a computing support representative (CSR) and notify the director of Customer Support, Office of Information Technology, of CSR appointments. CSRs will be knowledgeable about their units' computing environment and central resources and services. Units are responsible for compliance with risk evaluation procedures and the General Prevention Measures. CSRs are the first point of contact for unit personnel seeking problem resolution, information, and other assistance regarding computing and networking. CSRs will facilitate interaction between the unit and the Office of Information Technology and Internal Auditing regarding security issues.

General Prevention Measures:

http://www.security.gatech.edu/policy/general_measures.html

6.6. 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 “ftp” and “www.”) 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). Use of public services must not cause computer or network loading that impairs other services or impedes access by authorized users.

7. PROCEDURES AND SANCTIONS

7.1. Investigative contact

If anyone is contacted by a representative from an external law enforcement organization (District Attorney's Office, FBI, GBI, ISP security officials, etc.) that is conducting an investigation of an alleged violation involving Georgia Tech

computing and networking resources, they must inform the OIT Information Security Directorate at <http://www.security.gatech.edu/> and the Georgia Tech Office of Legal Affairs, 404-894-4812, immediately. Refer the requesting agency to the Associate Vice President and Associate Vice Provost for Information Technology; that Office will provide guidance regarding the appropriate actions to be taken. For routine matters, send e-mail to security@gatech.edu. For urgent matters, contact OIT Operations at 404-894-4669 and someone from the OIT Information Security Directorate will be paged immediately.

7.2. Responding to security and abuse incidents

All authorized users are stakeholders and share a measure of responsibility in intrusion detection, prevention, and response. At Georgia Tech the Associate Vice President and Associate Vice Provost for Information Technology has been delegated the authority to enforce information security policies and is charged with:

1. Implementing system architecture mandates, system protection features, and procedural information security measures to minimize the potential for fraud, misappropriation, unauthorized disclosure, loss of data, or misuse.
2. Initiating appropriate and swift action, using any reasonable means, in cases of suspected or alleged information security incidents to ensure necessary protection of Institutes resources, which may include disconnection of resources, appropriate measures to secure evidence to support the investigation of incidents, or any reasonable action deemed appropriate to the situation.

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, and (3) the OIT Information Security Directorate.

The OIT Information Security Directorate will coordinate the technical and administrative response to such incidents. Reports of all incidents will be forwarded to Student Affairs (for apparent policy violations by students) or the unit head (for employees), and to the Associate Vice President and Associate Vice Provost for Information Technology.

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 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 Affairs (for students) or the unit head (for employees) for investigation and appropriate action. 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 existing procedures established for employees and students.

7.7. Links to applicable policies and procedures:

Local, state, and federal laws http://www.security.gatech.edu/policy/law_library.html

Incident Response Guidelines

http://www.security.gatech.edu/architecture/incident_response_procedures.html

General Prevention Measures

http://www.security.gatech.edu/policy/general_measures.html

OHR Policies and Procedures

<http://www.admin-fin.gatech.edu/human/>

Institute Consulting Policy or the policy Access by External Entities to Institute Information Technology Resources

<http://www.security.gatech.edu/policy/xaccess.html>

Institute Data Access Policy –

http://www.security.gatech.edu/policy/data_access/home.html

Determination of Rights and Equities in Intellectual Property (Board of Regents Policy Manual, section 603.03)

<http://www.usg.edu/admin/policy/600.phtml#603.03>

<http://www.usg.edu/admin/policy/>

OIT Customer Support Center

<http://www.oit.gatech.edu/cs>

Georgia Tech Faculty Handbook (section 6.15.3.8(b))

<http://www.ohr.gatech.edu/policies/handbook.pdf>

Georgia Tech Academic Honor Code

<http://www.honor.gatech.edu>

Board of Regents Policy Manual (Use of System Materials)

<http://www.usg.edu/admin/policy/900.phtml>