H-190 COMPUTER, NETWORKING, AND INFORMATION RESOURCES

INTRODUCTION

1. The H-190 policy set constitutes Gateway Technical College's (Gateway or college) policy for the management of the college's computing, networking, and information resources. These resources include, but are not limited to, the central computing facilities, District-wide network, campus local area networks, email, nodal labs, classroom multimedia equipment, video conferencing equipment, access to the Internet, wireless access, voice mail, departmental and public computing facilities, scanners, printers, WebAdvisor, Blackboard, software, data, and related equipment and services.
2. Your use of Gateway computing and networking resources and information systems is governed by federal and state law; acceptable Internet use practices; Gateway policies; this Computing, Networking and Information Resources policy; and sub-policies under this policy set. Additionally, all Gateway policies regarding the appropriate use of Gateway resources and responsible personal conduct apply to your use of Gateway computing and networking resources and information systems.
3. **Your use of any of the college's computing, networking, and information resources constitutes your acceptance of this policy set.**

POLICY STATEMENT

1. Gateway provides computing and networking facilities and information resources to support its educational mission. These facilities include the central computer system, personal computer labs, communications networks, information systems and associated software, files, and data. Your access to and use of Gateway computing and network resources is a privilege that depends on your using the resources appropriately. In general, appropriate use means respecting the rights of other users, the integrity of the physical equipment and systems, and following all pertinent license and contractual agreements. Also, users must apply the highest level of ethical conduct to their use of computing, networking, and information resources. Users do not own accounts on Gateway computing systems, but are granted the temporary privilege of exclusive use.
2. Faculty, staff, and students may use the college's computing and networking resources for purposes related to their studies, their responsibilities for providing instruction and performing research, the discharge of their duties as employees, their official business with the college, and other Gateway-sanctioned or authorized activities. Personal use of these resources should be brief and limited. (See Policy H-190b - Digital Communications for additional information). In addition, residents of the District who have library cards may use computers in the public areas of Gateway libraries for word processing and Internet access, subject to compliance with all other rules and policies. The use of college computing and networking resources and information systems for any sort of solicitation is prohibited, absent prior written permission of a current officer of the college.
3. Computing resources may be used only for legal purposes and may not be used for any of the following purposes or any other purpose which is illegal, immoral, unethical, dishonest, damaging to the reputation of the college, inconsistent with the mission of the college, or likely to subject the college to liability. Impermissible uses (some of which may also constitute illegal uses) include, but are not limited to, the following:
   a. sending messages with the intent to frighten, intimidate, threaten, abuse or harass another person;
   b. defamation;

c. fraud or misrepresentation;
d. intentionally and without authorization:
    1) accessing, modifying, destroying, taking possession of, or copying data, computer programs or supporting documentation;
    2) disclosing restricted access codes or other restricted access information to unauthorized persons;
    3) modifying computer equipment;
    4) destroying or damaging a computer, computer system, or computer network;
e. sending messages while intentionally preventing or attempting to prevent the disclosure of one's own identity;
f. disruption or unauthorized monitoring of electronic communications;
g. unauthorized copying or transmission of copyright protected material;
h. use of the college's trademarks, logos, insignia, or copyrights without prior approval;
I. breaking into or attempting to break into Gateway systems, networks, or user accounts;
j. Unauthorized attempts to circumvent data protection schemes or uncover security loopholes. This includes creating and/or running programs that are designed to identify security loopholes and/or decrypt intentionally secure data.
k. using Gateway systems or networks as any part of an attempt to break into or attempt to break into other systems or networks;
l. downloading files or installing unauthorized software of any kind to computer hard drives;
m. unauthorized use of Internet, computer accounts, access codes (including passwords), or network;
n. use of identification numbers, user names, and/or authentication credentials (including email/Internet/Intranet addresses) assigned to others;
o. development or use of unapproved mailing lists;
p. use of computing facilities:
    1) for private business purposes unrelated to the mission of the college or to college life;
    2) for campaign or political purposes;
q. use which constitutes academic dishonesty;
r. violation of software license agreements;
s. violation of network usage policies and regulations;
t. violation of privacy;
u. accessing, displaying or sending obscene, pornographic, sexually explicit, or offensive material;
v. using any obscene, lewd or profane language or suggesting any lewd or lascivious act;
w. intentional or negligent distribution of destructive programs such as computer viruses;
x. creating, sending, or forwarding chain letters (messages that are forwarded many times to people who have not solicited the information);
y. permitting, encouraging, or directing another person to send a message prohibited by this policy from any Gateway computer or system under the user's control;
z. unauthorized solicitations such as creating and promoting products or services for sale;
aa. Use that is deemed unnecessary or excessive; use which facilitates violating other Gateway policies; and use which interferes or disrupts Gateway employees from performing their jobs.

ACCOUNT GUIDELINES

1. Once you are given access to computing resources at Gateway, you are responsible for any and all use made of those resources with your user identification. The following responsibilities apply to users accessing any of the college's computer and networking resources and information systems. The user is responsible for correct and sufficient use of the tools available for maintaining the security of information stored on each computer system.
   a. Computer accounts, usernames, passwords, and other types of authorization that are assigned to individual users may not be shared with others.
   b. The user should assign an obscure account password and change it frequently.
   c. The user should be aware of computer viruses and other destructive computer programs and take steps to avoid being a victim or unwitting distributor of these processes.
   d. No unauthorized persons may use Gateway computer and network resources. Authorized users include only Gateway employees, currently enrolled students, and residents of the District who have obtained library cards.
2. Be sensitive to the needs of others, and use only your fair share of computing resources. Collegiality requires:
   a. regular deletion of unneeded files from one's accounts on shared computing resources;
   b. refraining from overuse of connect time, information storage space, printing facilities, processing capacity, or network services;
   c. refraining from use of sounds and visuals which might be disruptive or offensive to others;
   d. refraining from use of computing resources in an irresponsible manner

ROLE OF THE LEARNING INNOVATION DIVISION

1. Responsible system maintenance may require that files be backed up, data cached, activity logs kept, and overall system activity monitored. In the process of these activities, Gateway staff may see your email/Internet/Intranet and files. The college shall also have access to and may monitor non Gateway computer and network resources used by Gateway employees in the course of their official duties.
2. Computers and networks are for use by authorized users only. Individuals using these systems are subject to having their activities on these systems monitored and recorded by system personnel. An account will also be inspected or monitored when:
   a. Activity from an account prevents access to the college's computing or networking resources by others.
   b. Activity from an account is disrupting or threatening the integrity of the network or network systems.
   c. General usage patterns indicate that an account is responsible for illegal activity.
   d. There are reports of violations of policy or law taking place.
   e. It appears necessary to do so to protect Gateway from legal liability.
   f. It is required by and consistent with law.
3. Whenever possible evidence of criminal activity is discovered, Gateway personnel will provide the evidence of such activity to law enforcement officials in accordance with state and federal statutes.

SANCTIONS FOR INAPPROPRIATE OR ILLEGAL USE OF COLLEGE COMPUTING, NETWORKING, AND INFORMATION RESOURCES

1. If you violate any of the Gateway computer and network use policies, you may be subject to disciplinary actions or the loss of privileges, including but not limited to, loss of access to computing resources as well as to Gateway disciplinary action up to and including termination and/or legal action.
2. Any offense that violates federal, state and/or local laws may result in the immediate loss of all Gateway computing privileges and will be referred to appropriate Gateway administrators and/or law enforcement authorities.
3. If Gateway Learning Innovation Division staff has evidence of misuse of computing and networking resources or information systems through a specific account, they will take the following steps to protect the systems, networks, and the user community:
   a. The suspected accounts will be suspended immediately pending the outcome of any investigation.
   b. The user's email/Internet/Intranet, files, disks, and/or other data and computer accessible storage media on the account will be inspected for evidence.
   c. Investigation of a student will be reported to the Student Success Division, and investigation of a faculty or staff member will be reported to that individual's supervisor when appropriate.
   d. Any violation will be reported to the appropriate authorities:
      1) Policy violations by a faculty or staff member will be reported to the individual's supervisor and to the Human Resources Department.
      2) Policy violations by a student will be reported to the campus dean and the executive vice-president/provost.
      3) Policy violations by a District resident will be reported to the campus dean and the executive vice president/provost.
      4) Illegal activity by a faculty or staff member, student, or District resident will be reported to the police and other appropriate law enforcement officials.

DATA SECURITY AND INTEGRITY

1. Gateway provides reasonable security against intrusion and damage to files stored on the central computing facilities. In the event that data have been corrupted as a result of intrusion, Gateway Learning Innovation Division staff should be notified immediately. Gateway also provides limited facilities for archiving and retrieving files specified by users and for recovering files after accidental loss of data. However, Gateway cannot be held accountable for unauthorized access by other users and is not liable for the inadvertent or unavoidable loss or disclosure of the contents of stored files.
2. Gateway recommends that students backup their own data on a regular basis. Gateway is not responsible for backup or any lost data.

Adopted: December 7, 2015 (responsible department: LID)
Supersedes: May 15, 2015 (Language from this policy moved to create H-190b, Digital Communications); May 11, 2009; July 15, 2002; January 14, 1998
Reviewed &/or Updated: