H - 190

H-190 COMPUTER, NETWORKING, AND INFORMATION RESOURCES

INTRODUCTION

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, email, classroom multimedia equipment, video conferencing equipment and systems, access to the Internet, wireless access, telecommunications, voice mail, scanners, printers, software (locally installed, network based, and cloud hosted), data, and related equipment and services.

Use of Gateway computing and networking resources and information systems is governed by federal and state law, all Gateway policies, and the Employee and/or Student Handbook. Use of any of the College's computing, networking, and information resources constitutes acceptance of this policy set.

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 and network activity monitored. In the process of these activities, Gateway staff may see your network traffic, digital activities, and/or files.
2. An account may 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 and/or security of the network or network systems.
   c. General usage patterns indicate that an account may be responsible for illegal activity.
   d. LID receives reports of alleged law or policy violations.
   e. It appears necessary to do so to protect Gateway from possible legal liability.
   f. It is required by and consistent with law.
3. Whenever evidence of criminal activity is discovered, Gateway will provide the evidence of such activity to law enforcement officials in accordance with state and federal statutes.

SANCTIONS FOR TECHNOLOGY POLICY VIOLATIONS

1. Violations of Gateway technology or security policy may result in 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 technology systems, resources, or policy violations 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 account files, digital storage, and/or other data and computer accessible storage media associated with the account will be inspected for evidence.

H - 190

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. violations will be reported to the appropriate authorities, who may take further action.

Sanctions apply to the following computer and network use policies:

a. D-110 - Telephone Usage
b. All H-190 sub-policies
c. H-199 - Printing and Photocopying Policy
d. J-150 - Usage of Copyrighted Computer Resources

Reviewed: 10/10/2024