3.4 Information Systems Ethics Policy

POLICY:

Gordon College's information system resources shall be made available only for appropriate uses, and will be used in a manner that protects both personal privacy and equitable availability across the College.

Rationale:

In order to further the College academic, research and service missions, a quality computing environment must be maintained. This environment ensures availability and equitable distribution of resources across the campus. Limited resources should not be used for purposes that are not directly related to the business of the College nor should they be used in a manner that would violate the personal privacy of faculty, staff or students associated with the College.

Appropriate Use:

Appropriate use of information systems is that which supports the College's objectives of teaching, research and extension of knowledge to the public.

Guidelines for the appropriate use of information systems:

a) Users shall not provide network or computer based services using College information systems without prior written approval and registration
b) Users shall not use information systems for promoting or maintaining a personal or private business or using College information resources for personal gain
c) Users shall not use information systems for unauthorized not-for profit business activities
d) Users shall not use information systems for creation, accession or transmission of pornographic, obscene, discriminatory, offensive, threatening, harassing, or intimidating materials
e) Users shall not use information systems for creation, accession, or participation in online gambling
f) Users shall not use information systems for activity or solicitation for political or religious causes
g) Users shall not use information systems to engage in harmful activities. Such activities include, but are not limited to, Internet Protocol (IP) spoofing, creating and/or propagating viruses, port scanning, disrupting services, damaging files, purporting or representing one's self as someone else, or intentional destruction of or damage to equipment, software or data.
h) Users shall not impede, interfere with, impair, or otherwise cause harm to other users' legitimate use of information systems
i) Users shall not use someone else's logon ID and password
j) Users shall not use information systems in such a way that violates local, state, or federal laws, including copyright, trademark, patent, or other intellectual property rights
k) Users shall be responsible for ascertaining that the use of information systems complies with all College policies
l) Users shall not use information systems in such a way that violates the College's contractual obligations, including limitations defined in software or other licensing agreements
m) Users shall not use information systems to transmit communications that are fraudulent, defamatory, harassing, obscene, threatening, that unlawfully discriminate or that are prohibited by law
n) Users shall not modify or remove computer equipment, software or peripherals without

proper authorization

o) Users shall not perform security scanning, probing or monitoring services without appropriate permission
p) Users shall not perform activities intended to circumvent security or access controls of any organization, including the possession or use of hardware or software tools intended to defeat software copy protection, discover passwords, identify security vulnerabilities, decrypt encrypted files, or compromise information security by any other means
q) Users shall not install or attach communication device(s) on computers or networks that allow off-campus devices to attach to the College network or computers without authorization
r) Users shall not disclose restricted College information
s) Users shall not engage in conduct that is inconsistent with the stated goals and mission of the College

College Access to User's Information (Privacy):

College access to a user's information systems includes any access by the College to approach, enter, or make use of the information stored on the College's information systems. To the extent permitted by law, the College seeks to preserve an individual's information or data from unsanctioned intrusion. Electronic and other technological methods must not be used to infringe upon a user's privacy.

Guidelines concerning access to user information:

a) The College seeks to preserve individual privacy, and does not routinely monitor individual usage; however, the College may in accordance with state and federal law, access and monitor information systems when:
    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 College or to protect the College from liability
    3) When necessary for the normal operation and maintenance of the information systems, or to identify or diagnose systems or security vulnerabilities and problems
    4) There are reasonable grounds to believe that a violation of law or a significant breach of College policy may have occurred
    5) An account appears to be engaged in unusual or unusually excessive activity as indicated by monitoring of general activity and usage patterns
    6) It is required by federal, state, or local law or administrative rules

b) Users understand that by attaching personal computing devices to the College information systems, they consent to the College's monitoring of their information systems for maintenance and security purpose

c) Electronic mail messages are not secure and therefore should not be assumed to be private.