Acceptable Use and Ethics

Information Technology Services

Acceptable Use Policy

1.0 Purpose

The purpose of this policy is to outline the acceptable use of computer and network equipment at the University of West Georgia. This policy is in place to protect the employees and students of the University of West Georgia. Inappropriate use exposes the University to risks including virus attacks, compromise of network systems and services, and legal issues.

2.0 Scope

This policy applies to all University of West Georgia faculty, staff and students, in addition to any guests who are authorized to use the University's computers and/or data network. Any computer, laptop, printer, or device that is capable of being connected to or transmitting data on the campus data network is subject to this policy. This includes equipment owned, leased, rented, or otherwise controlled or maintained by university employees and students, and other authorized users. Authorized users accessing university computing resources and the university data network from off campus sites through dial- up access, broadband access, or other connections are responsible for ensuring the security and integrity of system(s) they are using to establish said access.
Use of the University's computing and network resources constitute an acceptance of this policy.

3.0 Availability

These policies are freely available to everyone. Printed copies are available from Information Technology Services. Copies may also be obtained in both PDF and HTML formats, from the web at **http://www.westga.edu/policy/**. Adobe Acrobat reader is required to use the PDF format, and is freely available at **http://www.adobe.com/**.

4.0 Access and Use

Access and use of University of West Georgia computing and networking resources is regulated by this policy, the University of West Georgia policies, and other applicable local, state, and federal policies.

4.1 Authorized Users

Individuals who have been granted and hold an active and authorized account on a University of West Georgia computer or network or who access and use a University of West Georgia computer or network and abide by this policy are considered authorized users. Any currently enrolled student or employee may be an authorized user of University West Georgia computer or network resources. Accounts and the files associated with that account are deleted upon termination of employment or when a student is no longer enrolled. Student accounts are deleted after the drop/add period for the current term. Graduating students may continue to use their account for six months after graduation.

4.1.1 Authorized Use

Authorized use is that which is consistent with the academic, research and service goals of this institution and falls within the guidelines of this policy and the policy of the Board of Regents which states that property owned by the institution shall be used only for institutional purposes. According to Section 712.01 of the Board of Regents of the University System of

Georgia Policy Manual all computer and computer related resources are recognized as "valuable state assets" and therefore, property of the State of Georgia. Only people who have permission shall use such state assets.

Furthermore, Georgia Code 16-9-93 G makes using a computer without permission an act of theft:

a. Computer Theft. Any person who uses a computer or computer network with knowledge that such use is without authority and with the intention of:

   (1) Taking or appropriating any property of another, whether or not with the intention of depriving the owner of possession;
   (2) Obtaining property by any deceitful means or artful practice;
   or
   (3) Converting property to such person's use in violation of an agreement or other known legal obligation to make a specified application or disposition of such property

   shall be guilty of the crime of computer theft.

4.2 Privileged Users

Privileged users are authorized users that have administrative, special, or trusted access to the campus data network and campus computing resources including network devices, servers, student, faculty, and staff information systems and other systems that may contain sensitive data or information. Privileged users will maintain due diligence in carrying out day-to-day duties to prevent the loss of confidentiality and integrity of sensitive information and data.

4.3 Inappropriate Use

The following behaviors are considered a direct violation of this policy: harass, threaten or otherwise cause harm to a specific individual(s), whether by direct or indirect reference; impede, interfere with, impair or otherwise cause harm to the activities of others, to include the introduction of virus(s) onto the network or a computer; download or post to university computers, or transport across university networks, material that is illegal, proprietary, in violation of university contractual agreements or is otherwise damaging to the institution or individuals.

4.4 Unauthorized access

Users shall not attempt to guess or break another user's password. Attempting to gain access to University of West Georgia computers and networks to which you are not authorized is prohibited. A user may not use University of West Georgia computers to login or attempt to login to computers external to the University of West Georgia to which they are not authorized. It is a violation of this policy to read, alter, delete, or to change ownership or permissions of any other person's computer files, directories, or folders without proper authorization. This policy is applicable even if the system's operating system and/or security measures permit these acts. This also constitutes an act of "computer trespass" and is a violation of Georgia Code 16-9-93 G which states:

"Computer Trespass: Any person who uses a computer or computer network with knowledge that such use is without authority and with the intention of:

(1) Deleting or in any way removing, either temporarily or permanently, any computer program or data from a computer or computer network;
(2) Obstructing, interrupting, or in any way interfering with the use of a computer program or data;
or
(3) Altering, damaging, or in any way causing the malfunction of a computer, computer network, or computer program, regardless of how long the alteration, damage, or malfunction persists

shall be guilty of the crime of computer trespass."

If you suspect that your computer or system account has been compromised, and that your files have been tampered with you should contact Information Technology Services.

4.4.1 Unauthorized monitoring

Unauthorized monitoring of data or traffic on any network or system is expressly forbidden. Users shall not attempt to probe, scan, sniff, or test the vulnerability of a system or network without the express written permission from the university's Chief Information Officer.

4.5 Providing services

Users are not permitted to provide network or computer-based services using the University of West Georgia computers or networks without prior permission from the department responsible for the computers or networks in question. Examples of such services include, but are not limited to, FTP, WEB, IRC and peer-to-peer file sharing.

4.6 Sharing Passwords and Access

It is a violation of this policy for authorized users to share passwords, PINs, or any other means of access to the campus data network or campus computing resources.

Unauthorized disclosure of passwords is a violation of Georgia Code 16-9-93 G which states:

Computer Password Disclosure: Any person who discloses a number, code, password, or other means of access to a computer or computer network knowing that such disclosure is without authority and which results in damages (including the fair market value of any services used and victim expenditure) to the owner of the computer or computer network in excess of $500.00 shall be guilty of the crime of computer password disclosure.

4.7 Disruption of service

It shall be a violation of this policy to deliberately use a computer, laptop, or other device to disrupt or damage the academic, research, administrative, or related pursuits of another. Furthermore, such actions constitute an act of "computer trespass" according to Georgia Code 16-9-93 G:

(2) Obstructing, interrupting, or in any way interfering with the use of a computer program or data;
or
(3) Altering, damaging, or in any way causing the malfunction of a computer, computer network, or computer program, regardless of how long the alteration, damage, or malfunction persists

shall be guilty of the crime of computer trespass."

5.0 Harassment

The following acts constitute computer harassment if the actions are sufficiently severe, pervasive, or persistent so as to interfere with or limit the recipient's ability to work or to participate in or benefit from the services, activities, or opportunities offered by UWG: (1) Deliberately using a computer to harass, annoy, terrify, intimidate, threaten, or offend another person by transmitting obscene language, photographs, pictures, or other materials or threats of bodily harm to the recipient or the recipient's immediate family; (2) Repeatedly attempting to communicate with a recipient after the recipient has given reasonable notice that he or she does not desire such communication.

6.0 Privacy Issues

The University of West Georgia cannot guarantee the privacy of computer files, electronic mail, or other information stored or transmitted by computer unless special arrangements are made. Users should not place confidential files or information on computers or transmit confidential files or information through the University of West Georgia network system.

6.1 Invasion of Privacy

Use of a computer to invade or threaten the invasion of the privacy of anyone is prohibited.

Georgia Code 16-9-93 G states:

Computer Invasion of Privacy: Any person who uses a computer or computer network with the intention of examining any employment, medical, salary, credit, or any other financial or personal data relating to any other person with knowledge that such examination is without authority shall be guilty of the crime of computer invasion of privacy.

7.0 Legal Requirements and Institution Polices

Users of University of West Georgia computers and network systems are expected to abide by State and Federal laws that apply to the use of computers and computer resources. Users are also expected to abide by any institutional policies that apply to appropriate and ethical use of University of West Georgia computers or computer resources. This policy has been written and published in an attempt to make users aware of certain laws that apply to the usage of computers and computer resources. The Georgia Computer Systems Protection Act establishes certain acts involving computers as criminal and punishable by fines and/or imprisonment.

7.1 Individual Responsibilities and Expected Behaviors

Users of the University of West Georgia computer equipment and network systems are expected to understand this policy and abide by it. This policy is widely distributed and easily accessible, so lack of knowledge of this policy is not an excuse for failure to observe it. Questions regarding this policy can be directed to the Information Technology Services. Disregard for this policy may result in disciplinary actions as set forth in Section 8 of this document. In addition to local policy, users are expected to abide by the policies of the resources they may connect to over the Internet.

specific information such as system changes, policies and scheduled downtime. Additionally, valuable information is available at the University of West Georgia web site. System and network administrators may find it necessary to contact users regarding policy issues. If repeated attempts to contact an individual concerning a policy violation are unsuccessful, the system or network administrator may be forced to temporarily deactivate the account simply to compel the owner to make return contact.

The following behaviors are considered a direct violation of this policy: harass, threaten or otherwise cause harm to a specific individual(s), whether by direct or indirect reference; impede, interfere with, impair or otherwise cause harm to the activities of others, to include the introduction of virus(s) onto the network or workstation; download or post to university computers, or transport across university networks, material that is illegal, proprietary, in violation of university contractual agreements or is otherwise damaging to the institution; harass or threaten classes of individuals. Further explanations of these behaviors can be found at **http://policy.westga.edu/behavior.html**.

7.2 Personal Business Use and Advertising

The use of University of West Georgia computers and networking services for personal business is prohibited. The campus email system, web server, or any other University of West Georgia computer shall not be used to advertise, promote, or solicit private business.

The Board of Regents of the University System of Georgia states in Section 711.02 Business Enterprises that:

"Institutions of the University System shall not permit the operation of private business enterprises on their campuses, except as otherwise provided by contract. All business enterprises operated on a campus of an institution of the University System shall be operated as auxiliary enterprises and shall be under the direct management, control and supervision of the chief business officer of the institution."

7.3 Software and Intellectual Rights

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, right to privacy, and 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.

7.4 Use of copyrighted or licensed materials

Unauthorized copying of software is prohibited. Software installed on any University of West Georgia computer or network device must be accompanied with a valid license. Users may be asked to show a valid license agreement to ensure the legal use of software on University of West Georgia computers. Contact the department head responsible for the specific computer if you have any questions regarding licensing issues. Faculty, staff, and students who include copyrighted materials on their web pages or in any electronic format bear the responsibility for obtaining permission to use these materials from the author or creator.

8.0 Consequences of Violations

Violations of the policies contained in this document are subject to the same types of disciplinary action as violations of other University policies, or state or federal laws, including criminal prosecution in serious cases. All users are expected to be familiar with these policies and abide by them at all times. Penalties for violating this policy can include, but are not limited to:

-Suspension of University computing privileges
-Disconnection of the user's computer from the campus network
-Suspension from attending the University
-Expulsion from the University
-Criminal charges, if applicable
-Civil liability, if applicable

9.0 Definitions

Authorization is another word for permission, which is granted by the appropriate part of the University's governance and/or management structure, depending on the particular computers and/or network facilities involved and the way they are administered.
Authorized use of University owned or operated computing resources is use consistent with the education, research and service mission of the University, and consistent with this policy.
Authorized users are (1) current faculty, staff, and students of the University, (2) anyone connecting to a public information service; (3) others whose access furthers the mission of the University and whose usage does not interfere with other users' access to resources.
Hosts constitute any computer, laptop, server, printer, or device connected to the campus data network including those devices connected by wireless means.
University computers and network facilities, or University computing resources comprise all computers owned or administered by any part of the University of West Georgia or connected to the University's telecommunications facilities, including departmental computers, and also the University's computer network facilities accessed by anyone from anywhere.

10.0 Relevant Links

Student Handbook and Catalogs

Board of Regents of the University System of Georgia Policy Manual

Board of Regents of the University System of Georgia Policy Manual Section 711.02 Business Enterprises

Board of Regents of the University System of Georgia Policy Business Proceduce Manual Section 12 Data Governance and Management

Georgia Code 16-5-90 G - Cyber stalking Law

Georgia Code 34-1-7 G - Harassing or Threatening Activities

Georgia Code 16-9-90, 91, 92, 93, 93.1, 94 - Computer Crime, Computer Theft, Computer Trespass

http://www.lexisnexis.com/hottopics/gacode/Default.asp

11.0 Revision History

First Draft - 2003-12-03

2nd Draft -2004-11-15

3rd Draft -2008-10

Harrassment Section Updated - 2011-03-17

Carrollton
1601 Maple St
Carrollton, GA 30118
(678) 839-5000

Newnan
80 Jackson St
Newnan, GA 30263
(678) 839-2300

Connect