UNIVERSITY of West Georgia.

UWG PROCEDURE NUMBER: 8.1.1, Acceptable Use for Computers and Network
***Authority*: UWG Policy 8.1 (Technology and Use)**

All computers and computer related resources of the University of West Georgia are considered state assets and as such unauthorized/inappropriate use is prohibited.

NOTE: Use of the University's computing and network resources constitute an acceptance of this procedure.

Acceptable use of computers and the network includes use that supports the mission of the University and which does not expose the University to risks or legal issues. Unauthorized uses are set forth in the Georgia Code, Board of Regents policies, or as in these Procedures.

This Procedure applies to:

- All University of West Georgia faculty, staff and students
- Any guests or vendors 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
- Any equipment owned, leased, rented, or otherwise controlled or maintained by university employees and students, and other authorized users

The Chief Information Officer, pursuant to the authority of UWG Policy 8.1, establishes the following procedures for compliance with the Acceptable Use for Computers and Network.

A. Definitions.

1. ***Acceptable use*** – use consistent with the academic, research and service mission of the University that is otherwise consistent with the Acceptable Use for Computers and Network, UWG Policy 8.1, UWG Procedure 8.1.1., and the policies of the Board of Regents. Acceptable use includes accessing information only when necessary for the conduct of one's official duties.
2. ***Authorized account*** - any connection to a UWG computer or network 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
3. ***Authorized use of University owned or operated computing resources*** – see definition for "Acceptable Use" above.
4. ***Authorized users*** – anyone who has been given access to the University's data network or computers either through administrative approval or by way of contract, including (1) current faculty, staff, and students of the University who have been granted and hold an active and authorized account on a UWG computer or network, (2) graduating students for six months following graduation (3) vendors and guests whose access furthers the mission of the University and whose usage does not interfere with authorized users' access to resources
5. ***Harass or harassment*** - any action that is 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, including but not limited to: (1) the use of a computer to annoy, terrify, intimidate, threaten, or offend another person by transmitting or posting obscene language, photographs, pictures, or other materials or threats of bodily harm to the recipient or the recipient's immediate family; (2) repeated attempts to communicate with a recipient after the recipient has given reasonable notice that he

or she does not desire such communication; this definition addresses harassment in the context of computer and network use, and is not intended to replace any definition of harassment in the context of individual civil rights

6. ***Hosts***- any computer, laptop, server, printer, or device connected to the campus data network including those devices connected by wireless means
7. ***Malware*** – generally defined as malicious software or code designed to damage or disrupt computer terminals, networks, systems, but for the purposes of this Procedure malware will include any action through use of the computer that disrupts the academic, research, administrative, or related pursuits of any faculty member, staff, or student
8. **"This Procedure"** as referenced herein means UWG 8.1.1, Acceptable Use for Computers and Networks.
9. ***Unauthorized access***- Access to university computers or networks that has not been approved by administrative process or by contractual arrangement, which access includes, but is not limited to: (1) use of a password, PIN, or code by anyone other than the assigned individual, (2) entry to university networks to which you are not an authorized user, either from campus or off campus, (3) reading, deleting, or changing ownership or permissions of any other person's computer files, directories, or folders without their permission(4) any 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
10. ***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

B. Inappropriate Use.

Use of computers and the UWG network for University business may be considered acceptable use unless any person within the scope of this Procedure engages in the following prohibited behavior:

1. Harassment of a specific individual(s), whether by direct or indirect reference to that individual(s);
2. The intentional or negligent introduction of virus(s) or malware onto the university network or a computer;
3. Downloading or posting to university computers, or transporting across university networks, any material that is illegal, proprietary, in violation of university contractual agreements or is otherwise damaging to the institution or individuals;
4. Any action that constitutes unauthorized access;
5. Using the University of West Georgia computers or network to provide any technology-based service, including but not limited to, FTP, HTTP, and peer-to-peer file sharing, without prior permission from the Office of Information Technology Services;
6. Use of a computer, laptop, malware, or other device to disrupt or damage the academic, research, administrative, or related pursuits of another such that it effectively denies access to an educational benefit or opportunity;
7. Use of a computer to invade or threaten the invasion of the privacy of any person;
8. Use of University of West Georgia computers and networking services, including the use of the campus e-mail system, web server, or any other University of West Georgia computer for commercial use or the advertisement thereof beyond use that is transient and incidental and in accordance with Board of Regents policy or applicable law;
9. The violation of any federal, state, or local law, or the violation of any other university or Board of Regents policy on computer use;
10. Installing or using any software or program without the proper license or in violation of copyright laws; or
11. Repeated failure of any user to comply with requests or directives of his/her supervisor(s) or the Office of Information Technology concerning the use of computer resources.

C. Reporting Requirements.

Known violations of this procedure should immediately be reported to either your supervisor, the Chief Information Officer, or the UWG Ethics and Compliance Reporting Hotline at https://westga.alertline.com/gcs/welcome. The Chief Information Officer will take appropriate actions to secure the affected information and technology resources. When appropriate, the University's disciplinary and/or law enforcement authorities will coordinate with the University's Chief Information Officer to investigate and respond to alleged violations. Findings charging individuals with alleged violations of policies will be processed in accordance with the appropriate disciplinary procedures for faculty, staff and students, as outlined in the Faculty Handbook, the Student Code of Conduct, and other applicable policies and procedures.

D. Non-Compliance.

Failure to comply with these Procedures may result in disciplinary actions under applicable UWG policies or procedures, or referral to law enforcement officers as may be appropriate under Georgia law.

Penalties may include the following actions:
-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
-Other disciplinary action including payment of repair costs, or termination

All users should be aware that any information that is stored, created, or received by any university computer or through any university network is subject to inspection and review under Georgia's Open Records Act.

Issued by the Chief Information Officer, the 2 day of Dec, 2015.

Signature, Chief Information Officer

Reviewed by President:

Previous version dated: N/A

ADMINISTRATION & ADDITIONAL RESOURCES
Short Title: "Computer and Network Use"
Previous Versions: "Acceptable Use Policy" dated 3-17-2011
Oversight: Chief Information Officer
Additional Resources (Hot link provided where available):

- Student Handbook and Catalogs
- Board of Regents IT Handbook and Related Policies
  - http://www.usg.edu/policymanual/
  - http://www.usg.edu/information_technology_handbook/
  - http://www.usg.edu/policymanual/section11
- Georgia Code Sections - O.C.G.A., §§16-9-90 through 16-9-94 and O.C.G.A. § 34-1-7
  - http://www.lexisnexis.com/hottopics/gacode/Default.asp