Status **Active** PolicyStat ID **14074954**

UNIVERSITY OF WEST GEORGIA

Last Approved	07/2023
Effective	07/2023
Next Review	07/2026
Area	Information Technology/ Management (Procedures)
Chief Or Responsible Office	Information Technology Services

Acceptable Use for Computers and Network

Authority for Procedure granted by UWG PL #5001, Technology Use.

All Computers and computer-related resources, and Wireless Communication Device resources of the University of West Georgia (UWG) are state assets, and unauthorized/inappropriate use is prohibited.

NOTE: Use of University computers, network facilities, or computing resources constitutes an acceptance of this procedure.

Acceptable Use of computers and the network includes use that supports the University's mission and does not expose the University to risks or legal issues. Unauthorized uses are outlined in the Georgia Code, Board of Regents (BOR) policies, or as in this procedure.

This procedure applies to:

- All UWG faculty, staff and students.
- Any guests or vendors authorized to use the University's computers and/or data network.
- Any UWG host (i.e., computer, laptop, server, printer, or device) that connects (hard-wired or wireless) to or transmits 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.

A. 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 a University computer or

network;

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 UWG computers or networks 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 (ITS);
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 UWG computers and networking services, including the use of the campus e-mail system, web server, or any other UWG computer for commercial use or the advertisement thereof beyond use that is transient and incidental and per BOR policy or applicable law;
9. The violation of any federal, state law, or any BOR or University 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 their supervisor(s) or ITS concerning the use of computer resources.

1. Personal Use

Incidental personal use is an accepted and appropriate benefit of being associated with the University's technology environment. Appropriate incidental personal use of technology resources does not result in any additional cost to the University, does not interfere with an employee's execution of duties, and does not conflict with the mission of the University. Under no circumstances should incidental personal use of technology involve violations of the law or University policy or interfere with fulfilling an employee's University responsibilities.

B. Reporting Requirements

Known violations of this procedure should immediately be reported to your supervisor, the Chief Information Officer (CIO), or the UWG Ethics and Compliance Reporting Hotine. The CIO 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 CIO to investigate and respond to alleged violations. Findings charging individuals with alleged violations of policies will be processed following the appropriate disciplinary procedures for faculty, staff and students, as outlined in UWG's Employee Handbook, Faculty Handbook, Student Handbook and Wolf Code of Conduct, and/or other applicable policies and procedures.

C. Compliance

Failure to comply with this procedure may result in disciplinary actions under applicable UWG policies or procedures or referral to law enforcement officers as 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 actions, including termination

Any information stored, created, or received by any University computer or network is subject to inspection and review under Georgia's Open Records Act.

Definitions

Acceptable Use - authorized use consistent with the academic, research and service mission of the University that is otherwise· consistent with UWG PL #5001, *Technology and Use* and associated procedures and BOR policies. Acceptable use includes accessing information only when necessary for one's official duties.

Authorized Users - anyone 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.

Harassment - any action that is sufficiently severe, pervasive, or persistent 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, 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 reasonable notice is given that no such communication is desired may be considered Harassment. (see UWG PL #4002 Non-Discrimination and Anti-Harassment)

Malware - malicious software or code designed to damage or disrupt computer terminals, networks, or systems. For this procedure, malware includes any action through the computer that disrupts the

academic, research, administrative, or related pursuits of any faculty, staff, or student.

Unauthorized Access - access to University computers or networks not 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 by an authorized user, either on or off campus, (3) reading, deleting, or changing ownership or permissions of any other person's computer files, directories, or folders without permission, (4) any attempt to probe, scan, sniff, or test the vulnerability of a system or network without express written permission from the University's Chief Information Officer.

University Computers, Network Facilities, or Computing Resources - all computers and network facilities owned or administered by UWG or connected to the University's telecommunications facilities that anyone from anywhere accesses.

Guidelines and Related materials

- USG Information Technology Handbook (ITHB)

Approval Signatures

Step Description	Approver	Date
	Teresa D'Emilio	07/2023
Chief Information Officer	Kirk Inman [TD]	07/2023