Acceptable Use for Computing Systems and Services

Policy Summary

The George Washington University (hereinafter, "GW" or "the University") provides computing and network related technology and information resources ("Computing Systems and Services") to its community to support the university's academic and research mission as well as its business operations. The University's Computing Systems and Services are to be used in a responsible and ethical manner and consistent with university policy and the law.

This policy establishes the acceptable use of GW Computing Systems and Services to ensure that such resources are used for their intended purpose while respecting the rights of other computer users, the integrity of the technological infrastructure, and relevant license and contractual agreements.

In addition, this policy applies to the use of personally-owned computers and devices that connect to the campus network, and the use of off-campus computers (e.g.

computers located at a non-GW location that are being used as part of research projects and connect remotely to the university network services and information systems).

Who is Governed by this Policy

- All faculty, staff, students, contractors, consultants, temporary workers, and guests as well as those who represent themselves as being associated with the university and who make use of Computing Systems and Services ("Authorized Users").

Policy

Authorized Users must adhere to GW's standards of academic and professional ethics, as included in GW's codes of conduct and employee handbooks and considerate conduct in the use of Computing Systems and Services or any other computer system accessed by virtue of their affiliation with the University. Authorized Users agree to and are bound by this policy and all other applicable rules and regulations related to appropriate legal and ethical use of Computing Systems and Services.

The unauthorized use of Computing Systems and Services for personal or economic gain, political objectives, and any other activities that may jeopardize the University's reputation or regulatory compliance are prohibited.

I. Identification and Authorization

Authorized Users connected to Computing Systems and Services must be identified either through the physical location of an office computer or through an authorized university computer account. Authorized Users should log out of shared systems and take reasonable precautions to secure access to shared office computers.

II. Research

GW researchers obtain and share information and materials electronically that derive from a broad range of sources, including but not limited to organizations, federal agencies, websites, and specialized hardware and software. During the course of a project, GW researchers may unintentionally be at risk of exposure to malware, or other vulnerabilities, that may degrade Computing Systems and Services and put GW research information at risk for fraud, theft, or misappropriation. Researchers who are actively using Computing Systems and Services to perform research of this nature are responsible for completing all applicable paperwork to ensure that appropriate reviews and approvals are obtained before project initiation. Timely reporting

of planned research projects will ensure that research can be conducted unencumbered and that Authorized Users can proceed without experiencing a degraded state of resource availability.

Specifically, in the case of malware research, the researcher is expected to maintain specialized environments for containing and working with malware. Malware must not be allowed to communicate with systems outside of the university, without receiving prior specific approval from GW IT. Information regarding GW IT's requirements related to malware research can be made by contacting the IT Support Center.

III. Copyright and Intellectual Property

Authorized Users are prohibited from using Computing Systems and Services to violate the intellectual property rights of a third party. This includes copyright, trade secrets, patent or other intellectual property rights, as well as violation of similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products for which they are not appropriately licensed.

Additionally, Authorized Users are prohibited from using Computing Systems and Services to make or use unauthorized copies of copyrighted material including, but not limited to, music, movies, television shows, books, magazines, or software for which the university or the end user does not have an active license.

GW is required to adhere to the Digital Millennium Copyright Act and may report any instances of reported copyright violations to the copyright holders and associated trade groups upon request.

IV. Unauthorized Monitoring

Authorized Users must respect the privacy of others by refraining from inspecting, broadcasting, or modifying data without the consent of the individual or individuals involved, except as permitted as part of their employment, and then only to the extent necessary for employment.

Authorized Users may not seek out, examine, use, modify, or disclose, without authorization, Regulated or Restricted Information that is not related to their job function. Authorized Users are prohibited from executing any form of network monitoring to intercept data unless this activity is a part of the Authorized User's normal job/duty or pre-approved research.

V. False Identity and Misrepresentation

A GW NetID is a unique login name at the university. System roles and access permissions are granted through a NetID based on the Authorized User's unique access needs and responsibilities. For this reason, Authorized Users must not share login credentials (NetID, password and security question) with anyone.

Authorized Users are responsible for any and all activity conducted with their login credentials.Authorized Users of GW e-mail or other electronic communications, such as chat or text,

shall not employ a false identity, nor may any such electronic messaging be sent anonymously with the intent to deceive. This includes circumventing user authentication and unauthorized use.

In addition, Authorized Users are prohibited from using GW email to conduct personal business or any communication that is unrelated to GW. This includes but is not limited to using GW's email format, signature and branding.

Authorized Users are prohibited from emailing Restricted and Regulated Information to a personal email account (i.e., Gmail, Outlook, Yahoo!, etc.) or to any external unauthorized third party.

VI. Interference

Computing Systems and Services shall not be used for purposes that cause, or could reasonably be expected to cause, directly or indirectly, excessive strain on any computing facilities or unwarranted/unsolicited interference with others' use of Computing Systems and Services. Some examples of behaviors that are prohibited include: :

- Introducing honeypots, honeynets, or similar technology on the university network that entices hostile or excessive network traffic
- Port scanning or security scanning is expressly prohibited unless prior approval by GW IT has been granted
- Interfering with or denying service to any Authorized User (for example, a denial of service attack)
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, an Authorized User's session, via any means, locally or via the Internet
- Operating an unauthorized wireless access point

VII. Obscenity and Harassment

As outlined in GW's Equal Opportunity, Nondiscrimination, Anti-Harassment and Non-Retaliation Policy (/equal-opportunity-nondiscrimination-anti-harassment-and-non-retaliation), Computing Systems and Services may not be used to unlawfully discriminate against any person on the basis of protected characteristics or any other basis prohibited by federal law, the District of Columbia Human Rights Act, or other applicable law.

VIII. Enforcement and Penalties

Computer activity may be monitored by authorized individuals for purposes of maintaining system performance and security. In instances where individuals may be suspected of abuse of Computer Systems and Services, the contents of the individuals' user files may also be inspected by the university.

The university expects all members of the university community to adhere to and act in accordance with this policy. If an individual is found to be in violation of this policy, the university will take

disciplinary action, including the restriction and possible loss of network privileges. A serious violation could result in substantial consequences, up to and including suspension or termination from the university. Individuals are also subject to federal, state and local laws governing many interactions that occur on the Internet. These policies and laws are subject to change as state and federal laws develop and change.

Student violations of the above policies will be handled through the Office of Student Rights and Responsibilities; other violations will be referred, as appropriate, to the University Human Resources or the University Police Department.

Definitions

Authorized Users - All faculty, staff, students, contractors, consultants, temporary workers, and guests as well as those who represent themselves as being associated with the university and who make use of university computing systems and services.

Computing Systems and Services - Any equipment owned, operated or contracted by the university that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information electronically or via cloud-based systems, including printers, storage devices, computers, computer equipment, network equipment and systems and phone equipment and systems; and includes desktops, laptops, mobile phones, tablets, voice-over-internet protocol devices (VOIP), USB drives and other removable media, copiers, and the software that accesses, views, processes, transmits, stores or disposes of GW digital information.

For **Definitions of Public Information** and **Non-Public Information (Regulated Information** and **Restricted Information)** and guidance, please refer to the policy, Personal Information and Privacy (/personal-information-and-privacy-policy).

Related Information

Code of Student Conduct (https://business.gwu.edu/career-center/undergraduate/student-code-of-conduct)

Information Security Policy (/information-security)

Faculty Handbook (https://provost.gwu.edu/sites/g/files/zaxdzs626/f/downloads/Resources/GW_Faculty_Handbook-Final-Approved20150410.pdf)

Copyright Policy (/copyright)

Statement of Ethical Principles (https://compliance.gwu.edu/statement-ethical-principles)

Contacts

Contact	Phone Number	Email Address
IT Support Center (ITSC)	202-994-4948	ithelp@gwu.edu (mailto:ithelp@gwu.edu)

Responsible University Official: Chief Information Officer
Responsible Office: Information Technology
Last Reviewed: December 11, 2019
Non-compliance with this policy can be reported (https://compliance.gwu.edu/reporting) through this website.