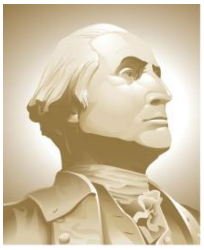

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Responsible University Official: Chief Information Officer
Responsible Office: Division of Information Technology
Last Revised Date: October 6, 2015

ACCEPTABLE USE FOR COMPUTING SYSTEMS AND SERVICES

Policy Statement

This policy governs the use of computing and network resources at the George Washington University. These resources provide access to university information services as well as the ability to communicate worldwide. Such access is a privilege extended to members of the university community as a benefit of their association with the university.

In general, acceptable use means respecting the rights of other computer users, the integrity of university resources under all pertinent legal, regulatory, license and contractual agreements. 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.

This document establishes specific requirements for the use of all computing and network-related information resources (”Computing Systems and Services”) at the university.

Reason for Policy

The purpose of this policy is to establish acceptable uses for computing and network-related information resources at the university. This policy applies to the use of university-owned and maintained computer equipment and networks. This policy also applies to personally owned computers and devices connected to the

campus network, and to off-campus computers that connect remotely to the university network services and information systems.

Computing and network resources are provided in support of the teaching, research, and public service mission of the university, and the administrative functions that support this mission.

The unauthorized use of university 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.

Who is Governed by this Policy

All faculty, staff, students, contractors, consultants, temporaries, as well as those who represent themselves as being associated with the university and who make use of university computing and/or information technology (IT) resources are required to read and understand this policy prior to using any university-owned and maintained computer equipment and networks. In some cases, university network users will need to agree to abide by this policy, in writing, prior to accessing some university systems and networks.

Table of Contents

Policy

Users must apply standards of academic and professional ethics and considerate conduct in the use of all university computing systems, services and networks or any other computer system accessed by virtue of their affiliation with the university. Users agree to and are bound by these and all other applicable rules and regulations related to appropriate legal and ethical use of university Computing Systems and Services, including the Code of Student Conduct and the Faculty Handbook.

I. Identification and Authorization

Individuals using university Computing Systems and Services must be identified either through the physical location of an office computer or through an authorized university computer account in the case of multiple user systems. Individuals may not knowingly access or use another person's computer account or knowingly allow another person to use his or her account. Users should log out of shared systems and take reasonable precautions to secure access to office computers. University Computing Systems and Services may not be used intentionally to misuse or gain unauthorized access to computing accounts or systems inside or outside of the university's systems.

II. Research

As a research institution, it is possible that GW researchers may be working with malware, network traffic, and specialized hardware and software that may degrade other users' ability to use and reach information resources. Researchers who are actively using the university systems, services or networks to perform research of this nature must report the nature of their work to the Division of Information Technology (DIT) for approval prior to beginning work. Timely reporting of this research will ensure that research can be conducted unencumbered and that no users experience 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 DIT.

III. Copyright and Intellectual Property

University users are prohibited from using computing and network services to

violate the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or 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.

University users are prohibited from unauthorized copying 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.

The university is required to adhere to the Digital Millennium Copyright Act ("DMCA") and may report any instances of reported copyright violations to the copyright holders and associated trade groups upon request.

IV. Unauthorized Monitoring

Computer 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.

University employees and others may not seek out, examine, use, modify, or disclose, without authorization Regulated or Restricted data that they need not access as part of their job function. Users are prohibited from executing any form of network monitoring which will intercept data not intended for the user's host, unless this activity is a part of the user's normal job/duty or pre-approved research.

V. False Identity

University users of e-mail or other electronic communications shall not employ a false identity, nor may any electronic messaging such as email, chat or text be sent anonymously with the intent to deceive. This includes circumventing user authentication and unauthorized use, or forging, of email header information.

A NetID is your unique login name at the university. System roles and access permissions are granted to a NetID based on the owner's unique access needs and responsibilities. For this reason, users must not share login credentials (NetID and password) with anyone. Users are responsible for any and all activity conducted with their login credentials.

VI. Interference

University computing 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 under this provision:

- 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 notification to the Division of IT is made.

- Interfering with or denying service to any user other than the user's host (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, a user's session, via any means, locally or via the Internet.

- Operate an unauthorized wireless access point.

VII. Obscenity and Harassment

University computing systems, services and networks may not be used in an obscene, harassing or otherwise inappropriate manner.

As outlined in the University Policy on Equal Opportunity, university-computing systems may not be used to unlawfully discriminate against any person on the basis of race, color, religion, sex, national origin, age, disability, veteran status, sexual orientation, or gender identity or expression, or on any other basis prohibited by applicable law.

VIII. Enforcement and Penalties

Computer activity may be monitored by authorized individuals for purposes of maintaining system performance and security. In instances when individuals are suspected of abuse of computer usage, the contents of user files may also be inspected upon the approval of DIT or someone designated by the Chief Information Officer (CIO) and the Office of the Senior Vice President and General Counsel ("OGC").

The university may take action to protect computer users from external or internal interference. The DIT or authorized individual designated by the Chief Information Officer (CIO), and OGC may authorize the termination of connections with external providers whose users interfere with the operation of university computing facilities.

At the discretion of the manager of the computer system or service in question, or designee, in collaboration with the appropriate authority, computer use privileges may be temporarily or permanently revoked pending the outcome of an investigation of misuse, or finding of violation of this policy.

Additional rules may be in effect at specific computer facilities at the discretion of the directors of those facilities.
Failure to comply with any of the provisions set forth in this policy may result in termination of network services, loss of computer lab privileges, prosecution by the university based on the student code of conduct, standard disciplinary procedures for faculty and staff, and/or criminal prosecution.

The Division of IT reserves the right to terminate any residential or lab computer connection without notice should it be determined that network traffic generated from said connection drastically inhibits or interferes with the use of the network by others. A reactivation fee may be charged if your network connection is terminated due to violations of this policy.

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

Computing Systems and Services	All computers owned, operated or contracted by the university and includes hardware, software, data, communication networks associated with these systems, and all allied services. The systems range from multi-user systems, desktop computers, tablets and phones, whether free standing or connected to networks.
Users	All those individuals with privileges on university computing systems and services.

For Definitions of **Public Information** and **Non-Public Information** (**Regulated Information** and **Restricted Information**) and guidance, please consult the Information Security Policy.

Related Information

Code of Student Conduct
Information Security Policy
Faculty Handbook
Copyright Policy

Contacts

Contact	Telephone	Email
IT Support Center (ITSC)	202-994-4948	ithelp@gwu.edu

Document History

- **Last Reviewed Date:** April 4, 2017
- **Last Revised Date:** October 6, 2015
- **Policy Origination Date:** October 6, 2015

Who Approved This Policy

Louis H. Katz, Executive Vice President and Treasurer

*This policy, as well as all **university policies**, are located on the **Office of Compliance and Privacy**'s home page.*