‹ Back to ETS Policies

Acceptable Use for Computer/Network Systems

Purpose

The Howard University computer and network infrastructure enriches the teaching, learning and research environment by providing students, faculty and staff convenient access to services such as:

- Electronic mail for communicating with other members of the University community, as well as with friends, relatives, colleagues and other correspondents throughout the world.
- On-line library catalogs, electronic journals, databases, and other sources of electronic information available through Internet.
- The Worldwide Web.
- Special-purpose programs on central computers.
- Administrative information systems.

The aim of these policies is to assure that the campus computer network and University computers continue to be effective resources for teaching, learning and research.

Applicability

This policy is intended to be compatible with the Howard University Student Code of Conduct and Judiciaries, the Howard University Faculty Handbook, and the Howard University Staff Handbook. In addition, to the maximum extent possible, this policy does not regulate content beyond what is stated by existing university policies which describe in detail the overall university policies, scope, applicability, responsibilities, and consequences. These policies include, but are not limited to, the following:

- Howard University Student Code of Conduct and Judiciaries
- Howard University Sexual Harassment Policy
- Howard University Code of Ethics
- Howard University Copyright Policy
- Applicable federal, state and local laws

This policy applies to:

- All University students, staff, and faculty and others granted use of Howard University’s information resources,

- All computing and data communications equipment owned, leased or operated by Howard University, and
- All equipment connected to the University's data network, regardless of ownership.
- All Individuals who use equipment connected to the University's data network, regardless of their affiliation with the University

Locally Defined and External Conditions of Use

Individual units within the University may define 'conditions of use' for information resources under their control. These statements must be consistent with this overall policy but may provide additional detail, guidelines and/or restrictions. Where such 'conditions of use' exist, individual units are responsible for publicizing and enforcing the additional regulations they establish. Where use of external networks is involved, policies governing such use also are applicable and must be adhered to.

Legal Process

The University does not exist in isolation from other communities and jurisdictions and their laws. Under some circumstances, as a result of investigations, subpoena or lawsuits, Howard University may be required by law to provide electronic or other records or other information related to those records or relating to use of information resources.

Policies

Users found to have violated any of the following policies will be subject to disciplinary action including, but not limited to reprimand, suppression, discharge, denial of access privileges, probations, academic expulsion and/or legal action.

Copyrights and Licenses

Users must respect copyrights and licenses to software and other on-line information.

- **Copying**
  All software protected by copyright must not be copied except as specifically stipulated by the owner of the copyright or otherwise permitted by copyright law. Protected software may not be copied except pursuant to a valid license or as otherwise permitted by copyright law.
- **Number of Simultaneous Users**
  The number and distribution of copies must be handled in such a way that the number of simultaneous users does not exceed the number of original copies purchased, unless otherwise stipulated in the purchase contract.

- **Copyrights**
  In addition to software, all other copyrighted information (text, images, icons, programs, videos, music, etc.) must be used in conformance with applicable law. Legitimately, copied material must be properly attributed. Plagiarism of computer information is subject to the same sanctions as apply to plagiarism in any other media.

- **Digital Millennium Copyright Act**
  The University complies with the Digital Millennium Copyright Act (1998). The University may terminate the network access of users who are found to repeatedly infringe the copyright of others and may take other disciplinary measures it deems appropriate.

Integrity of Information Resources

Users must respect the integrity of information resources.

- **Modification or Removal of Equipment**
  Computer equipment, software, or peripherals owned by the University must not be modified or removed without proper authorization.

- **Encroaching on Others' Access and Use of University Facilities**
  Users must not encroach on others' access and use of the University's network and computers. This includes but is not limited to:
  - Sending unsolicited bulk electronic mail or distributing unsolicited material though group communication channels
  - Sending chain-letters
  - Excessive printing
  - Using excessive network bandwidth
  - Running grossly inefficient programs when efficient alternatives are available
  - Modifying system facilities, operating systems, or disk partitions without proper authorization
  - Attempting to access private information without proper authorization
  - Attempting to crash or tie up University computers or networks
  - Damaging or vandalizing University computing facilities, equipment, software or computer files

- **Virus Protection**
  All computers connected to the University network must be protected by up-to-date anti-virus software. Viruses discovered on computers connected to the University network must be removed before infected computers are used for any other purpose.

- **Software Requirements**
  Computers with grossly outdated or inherently insecure software may not be connected to the University network.

- **Spyware**
  University computers often contain private information. Software or hardware that monitors web browsing, keyboard use or related activities must not be installed on University computers. Software installed on University computers must be selected cautiously. Some prohibited spyware is distributed as 'free' software, for which consumers agree to allow their activities to be monitored in exchange for use of the software.

  Use of spyware on personally owned computers connected to the University network is strongly discouraged. Use of programs to detect and expunge spyware is encouraged on all computers connected to the University network. Anti-spyware software is available to all from the iLab.

  This restriction is not intended to limit in any way the University's right to monitor any and all hardware or software owned by the University, or connected to the University network, for the purposes of preventing or investigating improper or illegal use of University systems, or preventing or investigating system problems or efficiencies.

- **Unauthorized Network Connections**
  Only officially assigned Internet Protocol (IP) numbers may be used for equipment connected to the University's data network. Official IP numbers are assigned by Information Systems and Services. Use of unassigned static IP numbers is prohibited.

  The Vice Provost and Chief Information Officer in Information Systems and Services must approve any device connected between a computer and the network.

- **Falsified Message Sources**
  Disguising or falsifying sources of electronic mail and other electronic communications with the intent of misleading, defrauding or harassing others is prohibited.

- **Computer Registration**
  Registering computing equipment connected to the University network is recommended. In the future, registration will be required.

- **Unauthorized or Destructive Programs**
  Users must not intentionally develop or use programs that disrupt others use of computers and networks, provide unauthorized access to private or restricted information, or damage software or hardware belonging to others.

Unauthorized Access

Users must refrain from seeking to gain unauthorized access to information resources or enabling unauthorized access.

- **Abuse of Computing Privileges**
  Users must not access computers, computer software, computer data or information, or networks

without proper authorization, or intentionally enable others to do so, regardless of whether the computer, software, data, information, or network in question is owned by the University. Abuse of networks to which the University belongs or computers at other sites connected to those networks will be treated as an abuse of University computing privileges.

- **Reporting Problems**
  Any defects discovered in system accounting or system security must be reported to appropriate system administrators and to Information Systems and Services so that steps can be taken to investigate and solve the problem.

- **Password Protection**
  All network accounts are password-protected. Account holders may be subject to both civil and criminal liability if they disclose passwords or otherwise make accounts available to others without permission of appropriate system administrators of Information Systems and Services.

Usage

- **Users must respect the rights of others.** University systems generally provide mechanisms for the protection of private information from examination by others. Attempts to circumvent these mechanisms in order to gain unauthorized access to the system or to another person's information are a violation of University policy and may violate applicable law. Authorized system administrators may access users' files at any time for maintenance purposes. System administrators will report suspected unlawful or improper activities to the proper authorities.

- **Unlawful Messages**
  Use of electronic communication facilities (such as e-mail, instant messaging, talk, chat rooms, threaded discussions or systems with similar functions) to send fraudulent, harassing, obscene, threatening, or other messages that are a violation of applicable federal, state or other law or University policy is prohibited.

- **Spam**

- Identical or nearly identical messages are sent to a large number of recipients (typically 25 or more, often thousands).

- The recipients have not granted deliberate, explicit, and still-revocable permission for the messages to be sent.

- The transmission and reception of the messages appear to the recipients to give a disproportionate benefit to the sender.

- **Bulk Email**
  In general, the use of the University's email system as medium for the bulk distribution of information is discouraged. Often mechanisms like targeted announcements on Banner or Blackboard are more direct and less disruptive than electronic mail.

On rare occasions, email may be the best mechanism to distribute information to large segments of the

University community. Approval of the Assistant Vice President for University Communications or a more senior executive-level administrator is required for messages sent to all students, all staff or both.

In addition, these guidelines should be followed:

- Messages should be plain text with no attachments. (If recipients require another kind of material, it can be posted at a website and links can be included in the message.)
- Distribution lists should be kept private. This can be done by listing recipients in Bcc: addresses instead of To: addresses or Cc: addresses.
- Timing and other details of bulk mailings to all students or all staff should be coordinated with the Assistant Vice President for University Communications.

- **Information Belonging to Others**
  Users must not intentionally seek or provide information on, obtain copies of, or modify data files, programs, or passwords belonging to other users, without the permission of those other users.

- **Content Filtering**
  The general policy of Howard University is to avoid filtering content passed through the University network. However, content filtering may occur in the following circumstances:

  - The University will filter network traffic if it is legally required to do so.
  - The University may block e-mail from sites known to send or transport excessive amounts of unsolicited bulk e-mail.
  - The University may scan e-mail for viruses, worms and other malicious programs. E-mail containing such programs may be refused either in whole or in part.
  - The University may block traffic likely to compromise the privacy of University information or the security and integrity of either internal or external networks.
  - The University may prioritize traffic passing through its network based on assumptions about traffic types and their requirements for quality of service.

- **Internet Content**
  The Howard University does not control information available over the Internet and is not responsible for Internet content. Internet users should be aware that Internet sites may contain offensive or controversial material. Users at workstations in open-access facilities such as the iLab are expected to show consideration for others. Full privacy in open-access spaces cannot be guaranteed. Others may see what an individual is viewing. Users should clear the screen of search results when finished. Users should consider the sensibilities of others in accessing networked resources at public access stations and using shared printers. Display of sexually explicit material in these settings may be considered intimidating, offensive, or hostile to others, and is strongly discouraged. Such activity may, therefore, constitute a violation of the University's Sexual Harassment Policy and University staff and/or Campus Police officers may be asked to intervene.

- **Political and Commercial Use**
  Howard University is a private, non-profit, tax-exempt organization and, as such, is subject to specific federal and District of Columbia laws regarding sources of income, political activities, use of property and similar matters. It also is a contractor with government and other entities and thus must assure proper use of property under its control and allocation of overhead and similar costs.
  - **Political Use**
    University information resources must not be used for partisan political activities where prohibited by federal, state or other applicable laws, and may be used for other political activities only when in compliance with federal, state and other laws and in compliance with applicable University policies.
  - **Commercial Use**
    University information resources should not be used for commercial purposes except as permitted under other written policies of the University or with the written approval of a University officer having the authority to give such approval. Any such commercial use should be properly related to University activities, take into account proper cost allocations for government and other overhead determinations and provide for appropriate reimbursement to the University for taxes and other costs the University may incur by reason of the commercial use.

System Administrator Responsibilities

The University delegates oversight of equipment to administrators such as deans, department chairs, administrative department heads, and principal investigators. These administrators are responsible for ensuring the adherence to the University's Acceptable Use Policy for equipment in their areas of responsibility. These persons may implement additional policies which are consistent with this overall policy but may provide additional detail, guidelines and/or restrictions.
Responsible administrators may designate other persons, known as *system administrators*, to manage computing and networking systems in their units. System administrators have additional responsibilities to the University as a whole for the systems under their oversight, regardless of the policies of their divisions. Responsible administrators have ultimate responsibility for the actions of the system administrators in their units.

System Administrators' University Responsibilities

System administrators have the following responsibilities for systems and networks they administer:

- Taking precautions against theft of or damage.
- Protecting the integrity and privacy of personal, financial, and other confidential information stored on systems and networks they administer.
- Executing all applicable hardware and software licensing agreements.
- Following appropriate practices for security and disaster recovery.

- Promulgating policies and procedures that govern services, access, and use of the systems they administer. At a minimum, this information should describe the data backup services, if any. A written document given to users or messages posted on relevant web pages shall be considered adequate notice.
- Reporting suspected legal violations, security threats or violations of University policy to appropriate University authorities.
- Cooperating with Information Systems and Services and with other system administrators, whether within or without the University, to find and correct problems caused by the use of systems under their control.

Policy Enforcement

System administrators are authorized to take reasonable actions to implement and enforce usage and service policies and provide for security.

Suspension of Privileges

System administrators may temporarily suspend access privileges if they believe it necessary to maintain the integrity of computer systems or networks. If legal violations, security threats, or violations of University policy are suspected, system managers should also inform appropriate University authorities. At a minimum, Information Systems and Services should be notified.

Vice Provost and Chief Information Officer Responsibilities

The Howard University's Vice Provost and Chief Information Officer shall be the primary contact for the interpretation, enforcement and monitoring of this policy and the resolution of problems concerning it. Any issues concerning law shall be referred to the Office of the General Counsel for advice.

Policy Interpretation

The Vice Provost and Chief Information Officer shall be responsible for interpretation of this policy, resolution of problems and conflicts with local policies, and special situations.

Policy Enforcement

Where violations of this policy come to his or her attention, the Vice Provost and Chief Information Officer is authorized to work with the appropriate administrative units to obtain compliance with this policy.

Inspection and Monitoring

Only the University's Vice Provost and Chief Information Officer or designate, can authorize the inspection of private data or monitoring of messages (including electronic mail) when there is reasonable cause to suspect improper use of computer or network resources.
The University's Vice Provost and Chief Information Officer may also authorize general inspection and monitoring to assure the security and stability of the network and systems connected to it. This may include, but is not limited to, monitoring and inspection to support activities such as:

- Assuring adequate quality of service for critical applications
- Detecting unauthorized use of the network
- Filtering content (as described above)
- Preventing or investigating system problems or efficiencies
- Assessing security vulnerabilities of computers connected to the network
- Preventing or investigating improper or illegal activities
- Compiling usage statistics

Consequences of Misuse of Computing or Network Privileges

Cooperation Expected

Users, when requested, are expected to cooperate with system or network administrators in any investigation of system abuse. Failure to cooperate may be grounds for suspension or cancellation of access privileges, or other disciplinary actions.
Users who feel they have been victims of abuse should contact Information Systems and Services.

Corrective Action

If system or network administrators have persuasive evidence of misuse of resources, and if that evidence points to the activities of an individual, they should pursue one or more of the following steps, as appropriate to protect individuals, networks and computer systems:

- Notify Information Systems and Services.
- In cases of grievous or dangerous violations, temporarily suspend or restrict computing or network access.
- With authorization from the Vice Provost and Chief Information Officer or designate, inspect private files, diskettes, tapes, and other computer-accessible storage media.

- Refer the matter for possible disciplinary action to the appropriate University unit, i.e., the Office of the Dean for Special Student Service for students, the supervisor for staff, and the dean of the relevant school or college for faculty or other teaching or research personnel.
- After consulting with the General Counsel, report evidence of criminal activity to appropriate authorities.