OFFICE OF HUMAN RESOURCES (OHR)
1650 Bedford Ave, Brooklyn, NY 11225
(718) 270-6910 (PHONE)
(718) 270-6909 (FAX)

Acceptable Use of Computer Resources

Introduction

CUNY's computer resources are dedicated to the support of the university's mission of education, research and public service. In furtherance of this mission, CUNY respects, upholds and endeavors to safeguard the principles of academic freedom, freedom of expression and freedom of inquiry.

CUNY recognizes that there is a concern among the university community that because information created, used, transmitted or stored in electronic form is by its nature susceptible to disclosure, invasion, loss, and similar risks, electronic communications and transactions will be particularly vulnerable to infringements of academic freedom. CUNY's commitment to the principles of academic freedom and freedom of expression includes electronic information. Therefore, whenever possible, CUNY will resolve doubts about the need to access CUNY computer resources in favor of a user's privacy interest.

However, the use of CUNY computer resources, including for electronic transactions and communications, like the use of other university-provided resources and activities, is subject to the requirements of legal and ethical behavior. This policy is intended to support the free exchange of ideas among members of the CUNY community and between the CUNY community and other communities, while recognizing the responsibilities and limitations associated with such exchange.

Applicability

This policy applies to all users of CUNY computer resources, whether affiliated with CUNY or not, and whether accessing those resources on a CUNY campus or remotely.

This policy supersedes the CUNY policy titled "CUNY Computer User Responsibilities" and any college policies that are inconsistent with this policy.

Definitions

"CUNY Computer resources" refers to all computer and information technology hardware, software, data, access and other resources owned, operated, or contracted by CUNY. This includes, but is not limited to, personal computers, handheld devices, workstations, mainframes, minicomputers, servers, network facilities, databases, memory, and associated peripherals and software, and the applications they support, such as e-mail and access to the internet.

"E-mail" includes point-to-point messages, postings to newsgroups and listservs, and other electronic messages involving computers and computer networks.

Rules for Use of CUNY Computer Resources

1. **Authorization.** Users may not access a CUNY computer resource without authorization or use it for purposes beyond the scope of authorization. This includes attempting to circumvent CUNY computer resource system protection facilities by hacking, cracking or similar activities, accessing or using another person's computer account, and allowing another person to access or use the user's account. This provision shall not prevent a user from authorizing a colleague or clerical assistant to access information under the user's account on the user's behalf while away from a CUNY campus or because of a disability. CUNY computer resources may not be used to gain unauthorized access to another computer system within or outside of CUNY. Users are

responsible for all actions performed from their computer account that they permitted or failed to prevent by taking ordinary security precautions.

2. **Purpose.** Use of CUNY computer resources is limited to activities relating to the performance by CUNY employees of their duties and responsibilities. For example, use of CUNY computer resources for private commercial or not-for-profit business purposes, for private advertising of products or services, or for any activity meant solely to foster personal gain, is prohibited. Similarly, use of CUNY computer resources for partisan political activity is also prohibited.

   Except with respect to CUNY employees other than faculty, where a supervisor has prohibited it in writing, incidental personal use of computer resources is permitted so long as such use does not interfere with CUNY operations, does not compromise the functioning of CUNY computer resources, does not interfere with the user's employment or other obligations to CUNY, and is otherwise in compliance with this policy.

3. **Compliance with Law.** CUNY computer resources may not be used for any purpose or in any manner that violates CUNY rules, regulations or policies, or federal, state or local law. Users who engage in electronic communications with persons in other states or countries or on other systems or networks may also be subject to the laws of those other states and countries, and the rules and policies of those other systems and networks. Users are responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular use.

   Examples of applicable federal and state laws include the laws of libel, obscenity and child pornography, as well as the following:

- Family Educational Rights and Privacy Act
- Electronic Communications Privacy Act
- Computer Fraud and Abuse Act
- New York State Freedom of Information Law
- New York State Law with respect to the confidentiality of library records
- Examples of applicable CUNY rules and policies include the following:
- Sexual Harassment Policy
- Policy on Maintenance of Public Order
- Web Site Privacy Policy
- Gramm-Leach-Bliley Information Security Program
- University Policy on Academic Integrity
- Information Security policies

4. **Licenses and Intellectual Property.** Users of CUNY computer resources may use only legally obtained, licensed data or software and must comply with applicable licenses or other contracts, as well as copyright, trademark and other intellectual property laws.

   Much of what appears on the internet and/or is distributed via electronic communication is protected by copyright law, regardless of whether the copyright is expressly noted. Users of CUNY computer resources should generally assume that material is copyrighted unless they know otherwise, and not copy, download or distribute copyrighted material without permission unless the use does not exceed fair use as defined by the federal

Copyright Act of 1976. Protected material may include, among other things, text, photographs, audio, video, graphic illustrations, and computer software.

5. **False Identity and Harassment.** Users of CUNY computer resources may not employ a false identity, mask the identity of an account or computer, or use computer resources to engage in abuse of others, such as sending harassing, obscene, threatening, abusive, deceptive, or anonymous messages within or outside CUNY.
6. **Confidentiality.** Users of CUNY computer resources may not invade the privacy of others by, among other things, viewing, copying, modifying or destroying data or programs belonging to or containing personal or confidential information about others, without explicit permission to do so. CUNY employees must take precautions to protect the confidentiality of personal or confidential information encountered in the performance of their duties or otherwise.
7. **Integrity of Computer Resources.** Users may not install, use or develop programs intended to infiltrate or damage a computer resource, or which could reasonably be expected to cause, directly or indirectly, excessive strain on any computing facility. This includes, but is not limited to, programs known as computer viruses, Trojan horses, and worms. Users should consult with the IT director at their college before installing any programs that they are not sure are safe.
8. **Disruptive Activities.** CUNY computer resources must not be used in a manner that could reasonably be expected to cause or does cause, directly or indirectly, unwarranted or unsolicited interference with the activity of other users. This provision explicitly prohibits chain letters, virus hoaxes or other intentional e-mail transmissions that disrupt normal e-mail service. Also prohibited are spamming, junk mail or other unsolicited mail that is not related to CUNY business and is sent without a reasonable expectation that the recipient would welcome receiving it, as well as the inclusion on e-mail lists of individuals who have not requested membership on the lists, other than the inclusion of members of the CUNY community on lists related to CUNY business. CUNY has the right to require users of CUNY computer resources to limit or refrain from other specific uses if, in the opinion of the IT director at the user's college, such use interferes with efficient operations of the system, subject to appeal to the President or, in the case of central office staff, to the Chancellor.
9. **CUNY Names and Trademarks.** CUNY names, trademarks and logos belong to the university and are protected by law. Users of CUNY computer resources may not state or imply that they speak on behalf of CUNY or use a CUNY name, trademark or logo without authorization to do so. Affiliation with CUNY does not, by itself, imply authorization to speak on behalf of CUNY.
10. **Security.** CUNY employs various measures to protect the security of its computer resources and of users' accounts. However, CUNY cannot guarantee such security. Users are responsible for engaging in safe computing practices such as guarding and not sharing their passwords, changing passwords regularly, logging out of systems at the end of use, and protecting private information, as well as for following CUNY's Information Security policies and procedures. Users must report incidents of Information Security policy non-compliance or other security incidents to CUNY's Chief Information Officer and Chief Information Security Officer, and the IT director at the affected user's college.
11. **Filtering.** CUNY reserves the right to install spam, virus and spyware filters and similar devices if necessary in the judgment of CUNY's Office of Information Technology or a college IT director to protect the security and integrity of CUNY computer resources. Notwithstanding the foregoing, CUNY will not install filters that restrict access to e-mail, instant messaging, chat rooms or websites based solely on content.
12. **Confidential Research Information.** Principal investigators and others who use CUNY computer resources to store or transmit research information that is required by law or regulation to be held confidential or for which a promise of confidentiality has been given, are responsible for taking steps to protect confidential research information from unauthorized access or modification. In general, this means storing the information on a computer that provides strong access controls

(passwords) and encrypting files, documents, and messages for protection against inadvertent or unauthorized disclosure while in storage or in transit over data networks. Robust encryption is strongly recommended for information stored electronically on all computers, especially portable devices such as notebook computers, Personal Digital Assistants (PDAs), and portable data storage (e.g., memory sticks) that are vulnerable to theft or loss, as well as for information transmitted over public networks. Software and protocols used should be reviewed and approved by CUNY's Office of Information Technology.

13. **CUNY Access to Computer Resources.**

CUNY does not routinely monitor, inspect, or disclose individual usage of its computer resources without the user's consent. In most instances, if the university needs information located in a CUNY computer resource, it will simply request it from the author or custodian. However, CUNY IT professionals and staff do regularly monitor general usage patterns as part of normal system operations and maintenance and might, in connection with these duties, observe the contents of web sites, e-mail or other electronic communications. Except as provided in this policy or by law, these individuals are not permitted to seek out contents or transactional information, or disclose or otherwise use what they have observed. Nevertheless, because of the inherent vulnerability of computer technology to unauthorized intrusions, users have no guarantee of privacy during any use of CUNY computer resources or in any data in them, whether or not a password or other entry identification or encryption is used. Users may expect that the privacy of their electronic communications and of any materials contained in computer storage in any CUNY electronic device dedicated to their use will not be intruded upon by CUNY except as outlined in this policy.

CUNY may specifically monitor or inspect the activity and accounts of individual users of CUNY computer resources, including individual login sessions, e-mail and other communications, without notice, in the following circumstances:

a. when the user has voluntarily made them accessible to the public, as by posting to Usenet or a web page;
b. when it is reasonably necessary to do so to protect the integrity, security, or functionality of CUNY or other computer resources, as determined by the college chief information officer or his or her designee, after consultation with CUNY's chief information officer or his or her designee;
c. when it is reasonably necessary to diagnose and resolve technical problems involving system hardware, software, or communications, as determined by the college chief information officer or his or her designee, after consultation with CUNY's chief information officer or his or her designee;
d. when it is reasonably necessary to protect CUNY from liability, or when failure to act might result in significant bodily harm, significant property loss or damage, or loss of significant evidence, as determined by the college president or a vice president designated by the president, after consultation with the Office of General Counsel and the Chair of the University Faculty Senate (if a CUNY faculty member's account or activity is involved) or Vice Chair if the Chair is unavailable;
e. when there is a reasonable basis to believe that CUNY policy or federal, state or local law has been or is being violated, as determined by the college president or a vice president designated by the president, after consultation with the Office of General Counsel and the Chair of the University Faculty Senate (if a CUNY

faculty member's account or activity is involved) or Vice Chair if the Chair is unavailable;

f. when an account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns, as determined by the college president or a vice president designated by the president and the college chief information officer or his or her designee, after consultation with CUNY's chief information officer or his or her designee, the Office of General Counsel, and the Chair of the University Faculty Senate (if a CUNY faculty member's account or activity is involved) or Vice Chair if the Chair is unavailable; or

g. as otherwise required by law.

In those situations in which the Chair of the University Faculty Senate is to be consulted prior to monitoring or inspecting an account or activity, the following procedures shall apply: (i) the college president shall report the completion of the monitoring or inspection to the Chair and the CUNY employee affected, who shall also be told the reason for the monitoring or inspection, except where specifically forbidden by law; and (ii) if the monitoring or inspection of an account or activity requires physical entry into a faculty member's office, the faculty member shall be advised prior thereto and shall be permitted to be present to observe, except where specifically forbidden by law.

A CUNY employee may apply to the General Counsel for an exemption from some or all of the circumstances under which CUNY may inspect and monitor computer resource activity and accounts, pursuant to subparagraphs (a)-(f) above, with respect to a CUNY computer resource used solely for the collection, examination, analysis, transmission or storage of confidential research data. In considering such application, the General Counsel shall have the right to require the employee to affirm in writing that the computer resource will be used solely for the confidential research. Any application for exemption should be made prior to using the computer resource for the confidential research.

CUNY, in its discretion, may disclose the results of any general or individual monitoring or inspection to appropriate CUNY personnel or agents, or law enforcement or other agencies. The results may be used in college disciplinary proceedings, discovery proceedings in legal actions, or otherwise as is necessary to protect the interests of the University.

In addition, users should be aware that CUNY may be required to disclose to the public under the New York State Freedom of Information Law communications made by means of CUNY computer resources in conjunction with University business.

Any disclosures of activity of accounts of individual users to persons or entities outside of CUNY, whether discretionary or required by law, shall be approved by the General Counsel and shall be conducted in accordance with any applicable law. Except where specifically forbidden by law, CUNY employees subject to such disclosures shall be informed promptly after the disclosure of the actions taken and the reasons for them.

The Office of General Counsel shall issue an annual statement of the instances of account monitoring or inspection that fall within categories (d) through (g) above. The statement shall indicate the number of such instances and the cause and result of each. No personally identifiable data shall be included in this statement.

See CUNY's Web Site Privacy Policy for additional information regarding data collected by CUNY from visitors to the CUNY website at www.cuny.edu.

14. **Enforcement.** Violation of this policy may result in suspension or termination of an individual's right of access to CUNY computer resources, disciplinary action by appropriate CUNY authorities, referral to law enforcement authorities for criminal prosecution, or other legal action, including action to recover civil damages and penalties.

    Violations will normally be handled through the university disciplinary procedures applicable to the relevant user. For example, alleged violations by students will normally be investigated, and any penalties or other discipline will normally be imposed, by the Office of Student Affairs.

    CUNY has the right to temporarily suspend computer use privileges and to remove from CUNY computer resources material it believes violates this policy, pending the outcome of an investigation of misuse or finding of violation. This power may be exercised only by the President of each college or the Chancellor.

15. **Additional Rules.** Additional rules, policies, guidelines and/or restrictions may be in effect for specific computers, systems, or networks, or at specific computer facilities at the discretion of the directors of those facilities. Any such rules which potentially limit the privacy or confidentiality of electronic communications or information contained in or delivered by or over CUNY computer resources will be subject to the substantive and procedural safeguards provided by this policy.
16. **Disclaimer.** CUNY shall not be responsible for any damages, costs or other liabilities of any nature whatsoever with regard to the use of CUNY computer resources. This includes, but is not limited to, damages caused by unauthorized access to CUNY computer resources, data loss, or other damages resulting from delays, non-deliveries, or service interruptions, whether or not resulting from circumstances under the CUNY's control.

    Users receive and use information obtained through CUNY computer resources at their own risk. CUNY makes no warranties (expressed or implied) with respect to the use of CUNY computer resources. CUNY accepts no responsibility for the content of web pages or graphics that are linked from CUNY web pages, for any advice or information received by a user through use of CUNY computer resources, or for any costs or charges incurred by a user as a result of seeking or accepting such advice or information.

    CUNY reserves the right to change this policy and other related policies at any time. CUNY reserves any rights and remedies that it may have under any applicable law, rule or regulation. Nothing contained in this policy will in any way act as a waiver of such rights and remedies.

Last Updated: 8/11/08