Policy Number: **C8.2**

Policy Name: **CODE OF CONDUCT FOR COMPUTER AND NETWORK USE**

I. Introduction

The computing, network, and information resources of the Rochester Institute of Technology are intended to support the mission of teaching, scholarly activity, and service for the University's students, faculty and staff. Appropriate use of computing and networking facilities by members of RIT's academic community should always reflect academic honesty and good judgment in the utilization of shared resources, and observe the ethical and legal guidelines of society. This document constitutes the Rochester Institute of Technology's policy for the proper use of all computing and network resources.

RIT's computer and network facilities provide access to a wide variety of on and off campus resources. This privilege of access requires individual users to act in an ethical manner and as a result imposes certain responsibilities and obligations. It is the responsibility of every user to respect the rights, privacy, and intellectual property of others, respect the integrity of the resources, and abide by all local, state, and federal laws and regulations.

This document outlines the user privileges and responsibilities as well as the guidelines and procedures for the responsible use of the RIT computer systems and networks. It is intended to allow for the proper use and management of these facilities, provide protection of users' rights, ensure reasonable access, and provide guidelines for accountability. It applies not only to RIT computers and networks, but also to computers attached to RIT's networks in any way.

II. Definitions

To avoid ambiguity, the following definitions are supplied:

A. **User -** Anyone who uses computing or network facilities.

B. **Authorized University User** - Anyone who has followed account application procedures and has been granted access to any or all of the computing or network resources of the Rochester Institute of Technology for reasons consistent with the mission of the university, and consistent with this policy.

C. **University Computing Resources** - Any computing, network, or software system donated to or purchased by the University or by a grant that is resident at the University.

D. **University Network** - The network of the University comprising the physical components such as cable, switches, telecommunications equipment, wireless hubs, routers, Virtual Private Network (VPN) concentrators, dial-up access points, as well as the Internet and Internet2 connection points. The University network also has logical components such as IP addresses, directory services, routing, and connectivity to computing resources.

E. **University Network Connections** - Any computer or device using an Internet address assigned to RIT or that is connected to a physical or wireless access point is considered to be connected to the University network.

F. **Personal Computing Resources** - Personal resources such as PCs, information appliances, networking equipment, etc. which have been purchased and are owned by an Authorized University User and are connected to the University network.

G. **Special Access** - Access to resources on a system that could be used to alter the behavior of the system, or to access accounts on the system, either directly or indirectly. Examples are UNIX "root" or Windows "Administrator or System."

H. **System Owner** - The system owner is the person with the authority to designate or use special access account privileges.

I. **System or Network Administrator** - The person responsible for maintaining the authentication used by the system or network, controlling authorized use, and maintaining system and network integrity and audit trails.

J. **Secure Systems** - Any hardware or software system whose use is restricted to a subset of the community of legitimate RIT users.

III. Relationship to Other University Policies

A. **University Policies** - Many issues addressed in this Code of Conduct relate to existing University policies, including (but not limited to) the University's policies on privacy, intellectual property, and prohibition of discrimination and harassment (found elsewhere in this Manual). This Code is intended to supplement and clarify the guidelines laid out in those policies as they apply to use of computer systems and electronic resources, not to supersede them.

B. **Other Computer Use Policies** - Campus units that operate their own computers or networks are encouraged to add, with the approval of the unit administrator, additional guidelines that supplement, but do not lessen, the intent of this policy or other University policies. In such cases, the unit administrator will inform users within the unit and will provide a copy of the unit-level policy to the Chief Information Officer and to the Information Security Officer.

IV. User Privileges and Responsibilities

A. **Privacy** - The University's "Privacy Policy" (C7.0) recognizes that "Individual privacy and security are highly valued by our society," but "must be balanced by the other community enumerated values and needs." Within this understanding, the RIT community is assured that the privacy of such "personal property" as "written communications intended by their creator to be private including those transmitted or preserved in paper, electronic, or other media" will be protected, although it cannot be completely guaranteed.

The "Privacy Policy" also recognizes that members of the RIT community have a responsibility to cooperate with authorized searches and seizures in emergencies and in circumstances of

probable cause. In such instances, including those involving RIT computer and network use, the search and/or seizure of personal property or personal communications will be executed only on the authorization of an official identified in the "Privacy Policy." Cooperation with the search or seizure of one's personal property or personal communication does not of itself imply one's own misuse or abuse of RIT computers or network; the search or seizure may be deemed necessary because of misuse or abuse elsewhere in the RIT system or in systems to which the RIT system is connected or affiliated. For example, scanning and pattern-matching of incoming or outgoing e-mail may be necessary to remove computer viruses, to locate the sources of spam, or to respond to legitimate internal or external requests for investigation. In all instances of investigation into personal computing and network use, individuals are protected to the extent possible by the provisions of the "Privacy Policy."

B. **Freedom from Harassment** - The RIT "Policy Prohibiting Discrimination and Harassment" (C6.0) defines "harassment" as unwelcome "conduct, communication, or physical contact" which has the effect of either "unreasonably interfering with" another's work, activities, or participation, or of "creating an intimidating, hostile or abusive environment" for an RIT employee or student. Members of the RIT community are assured that electronic communications that appear to have one or more of these effects are prohibited and will be investigated. This prohibition includes all obscene, defamatory, threatening, or otherwise harassing messages.

Correspondingly, members of the RIT community have the obligation not to use the RIT computing systems and network in such a way as to be reasonably judged to produce one or another of the above effects, whether intentionally or unintentionally. Such alleged or real misuse is covered by the provisions of this Code of Conduct as well as by the "Policy Prohibiting Discrimination and Harassment" (C6.0).

C. **Intellectual Property** - The RIT policy on "Intellectual Property" (C3.0) deals in a detailed and exhaustive way with the rights of RIT employees as creators and owners of intellectual property. The privilege of creating and owning intellectual property as outlined in that policy is fully recognized by this Code of Conduct

However, where a violation of the "Intellectual Property Policy," or of the intellectual property rights of creators or owners beyond the RIT campus, is alleged to have occurred through student or employee misuse of the RIT computing systems and network, such alleged misuse will be investigated and, if proved, sanctioned.

For example, RIT users must not distribute copyrighted or proprietary material without written consent of the copyright holder, nor violate U.S. copyright or patent laws concerning computer software, documentation, or other tangible assets. Users should assume that any software or other electronic materials or media are copyright protected, unless the author(s) explicitly states otherwise.

D. **Freedom of Expression** - In general, all members of the RIT community – students and employees alike – enjoy freedom of expression in the normal course of their activity. This freedom is both assured by numerous University policies and constrained by specific provisions

of certain RIT policies, such as those noted herein (C3.0, C6.0, C7.0 and C10.0) as well as by specific provisions of this Code of Conduct. The constraints are, as in civil law, imposed only for the sake of the common good and the rights of individuals.

Consequently, members of the RIT community have the responsibility to use RIT's electronic resources in ways that respect the rights of others and permit our common electronic resources to be equitably shared. Since free and civil discourse is at the heart of a university community, users should communicate in a manner that advances the cause of learning and mutual understanding.

RIT reserves the right to restrict or deny access to its computing resources to those whose use of them is not consonant with the mission of the university.

V. Responsible Use of Resources

In exchange for the privileges associated with membership in the RIT computing community, users assume the responsibility to use the community's resources in a responsible and professional manner. The following paragraphs (A.-G.) highlight a non-exhaustive list of specific responsibilities. Questions about the appropriateness of any use of resources should be directed to the staff of the Division of Information and Technology Services or to the systems personnel responsible for the resource in question.

A. **Access to Secure Systems**

1. **Passwords and similar authorization information** - Passwords are the primary way in which users are authenticated and allowed to use the community's computing resources. One should not disclose one's password(s) to any individual, including a faculty or staff member, unless the person is a properly authorized system administrator performing account maintenance activities for which the password is required. Similarly, one should not disclose other identifying information (e.g., PIN numbers) used to access specific system information. Authorized users are held accountable for violations of this Code of Conduct involving their accounts.

2. **Unauthorized use of resources** - One must not allow others to make use of one's account(s) or network access privileges to gain access to resources to which they would otherwise be denied.

3. **Circumventing or compromising security** - Users must not utilize any hardware or software in an attempt to compromise the security of any other system, whether internal or external to the RIT systems and network. Examples of prohibited activities include (but are not limited to) Trojan horses, password crackers, port security probes, network snoopers, IP spoofing, and the launching or knowing transmission of viruses or worms.

B. **Self-Protection** - Any member of the RIT community who attaches a computer to the RIT network must take measures to ensure that the computer is protected against compromise by an internal or external attack. In this context, reasonable measures include the installation and maintenance of virus detection and eradication software, care in opening e-mail message attachments, vigilance when visiting web sites and adhering to published system configuration

and management standards.

C. **Commercial Activity** - No member of the RIT community may use an RIT computing account or any communications equipment that is owned or maintained by RIT to run a business or commercial service or to advertise for a commercial organization or endeavor. Use of RIT's computer systems and networks for the personal promotion of commercial goods or services is strictly prohibited. RIT employees who are engaged in professional consulting for-a-fee relationships may use RIT's computing and network resources to correspond with existing clients, but not to advertise or promote their consulting practice.

D. **Personal Use of RIT Resources** - In general, the use of RIT's computing and network resources to promote commercially-related activities or events that have no direct relationship to RIT's mission is not permitted. Occasional personal use of these resources, for example, to promote a single fund-raising event or activity, to sell a used item within the RIT community, or to offer RIT colleagues the opportunity to rent a house may be permitted at the tacit discretion of the Chief Information Officer.

E. **Communication with Government Officials** - E-mail communications with government officials must abide by RIT's guidelines for political activities as outlined in policy C10.0. Individuals wishing to address a legislative issue on behalf of the university should consult with the Office of Government and Community Relations before sending such communications using RIT's network.

F. **Harmful Activities** - One must not use one's privileges as a member of the RIT computing community to cause harm to any individual or to harm any software or hardware system, whether internal or external to RIT. Examples of harmful activities, in addition to those noted elsewhere in this Code, include:

1. Intentional damage

    - Disabling others' computers
    - Compromising security
    - Disabling or corrupting software systems
    - Destroying, altering, or compromising information integrity (e.g., student records, personnel information, etc.)

2. E-mail spamming
3. Threatening or intimidating e-mail, newsgroup postings, or web sites.
4. Denial of service attacks (e.g., making it difficult or impossible for others to use the network effectively and efficiently).

G. **Illegal Activities** - For the protection of the RIT computing community as a whole, it is imperative that all members refrain from any conduct that is illegal. Illegal activities that are prohibited include (but are not limited to):

1. Copyright infringement, including publishing copyrighted material such as papers,

software, music, musical scores, movies, and artistic works. It is irrelevant whether or not any profit is made from such distribution; the mere fact of providing uncontrolled access to such material is illegal.
2. Divulging information that is confidential or proprietary information.
3. Misrepresentation of one's identity to gain access to systems, software, or other services to which one does not have authorized access.

VI. RIT Rights

Users should be aware that their use of RIT's computing and network resources is not completely private. However, in all RIT operations discussed in the following paragraphs, individual rights of privacy will be preserved to the extent possible and compatible with the nature of the operation. As an institution, RIT retains the following rights with respect to its computing and network resources:

A. **Allocation and Control of Access to Resources** - Those responsible for maintaining RIT's information technologies and resources have the right to allocate resources in ways appropriate to the achievement of RIT's overall mission. They also may control access to its information and the devices on which it is stored, manipulated and transmitted in accordance with the policies of the University, the laws of the State of New York and the United States.

B. **Usage Monitoring and Inspection of Files** - While RIT does not routinely monitor individual usage, the normal operation and maintenance of the University's computing and network environment require the backup and caching of data, the logging of usage data, the monitoring of usage patterns and other such activities that are necessary for maintaining network availability and performance. RIT system and network administrators may review this data for evidence of violation of law or policy.

When necessary to ensure network availability and performance, or to respond to an alleged violation of law or policy, system and network administrators may monitor the activities and inspect the files of specific users on their computers and networks.

C. **System and Network Administration Access** - A system administrator may access others' files for the maintenance of network computer and storage systems. Similarly, for the maintenance or security of networks, a network administrator may access others' files and data on network devices or in transit.

D. **Security Procedures** - Departments are responsible for educating the users of university-owned desktop computers and providing a reasonable level of security for sensitive information. It is advisable that departments with their own local area networks or a significant number of desktop computers appoint a contact person and identify this person to Information and Technology Services. The contact person should be knowledgeable about the department's computing environment and about central resources and services. This position will serve:

1. As the first point of contact for unit personnel seeking problem resolution, information, and other assistance regarding computing and networking, and

2. To facilitate interaction between the unit and Information and Technology

Services staff on security matters. As a facilitator of communication between the unit and Information and Technology Services on security matters, or alleged abuses or related issues.

VII. Reporting, Investigations, and Sanctions

A. **Reporting Violations of this Code** - For this Code to be effective, all members of the RIT computing community must be alert to possible violations. If a member of the community suspects that another community member is abusing his or her privileges or is engaged in activities forbidden by this policy, it is that member's responsibility to report this to either ITS personnel or the administrative staff in charge of the affected systems. In all cases, suspected violations of this Code of Conduct should be reported to the electronic mail address abuse@rit.edu. Users should retain any other information that could be helpful for investigative purposes, such as harassing e-mail messages, dates and times of unauthorized access, and header lines.

B. **Investigation of Suspected Violations** - Reports of suspected violations of this Code of Conduct are investigated by the designated professional staff of the Division of Information and Technology Services in consultation with the RIT Information Security Officer and/or Public Safety if necessary. Confirmed violations will be brought to the attention of the violators and, where a confirmed violation is serious or persists, a restriction may be imposed, temporarily or permanently, by the University. Violators of statutory law will be turned over to Public Safety.

C. **Sanctions** - RIT may impose a range of penalties on users who violate the policies regarding the usage of university computing resources. For example, RIT may suspend computer and network privileges of an individual for reasons relating to the safety and well-being of other members of the campus community, or relating to the preservation and integrity of university property. Access will be restored when positive conditions can be reasonably assured, unless access is to remain suspended as a result of formal action imposed through the normal disciplinary processes of the University. Appeals will follow the normal RIT Student Conduct Process.

VIII. Questions and Interpretations

Questions about the appropriateness of any use of resources should be directed to the staff of the Division of Information and Technology Services or to the systems personnel responsible for the resource in question.

Responsible Office: Global Risk Management/Division of Information and Technology Services

Effective Date: Approved April 6, 1988

Policy History:
Revised April 24, 2002
Edited October 2010