NYIT COMPUTING CODE OF RESPONSIBLE TECHNOLOGY USAGE

New York Institute of Technology (hereinafter referred to as the College) provides resources for the academic research and instructional and business purposes of its faculty, staff, students and university affiliates. These resources include telephone and computer equipment, software, networks and accounts. Any and all information or communication transmitted by, received from or stored in these systems are property of the College and are provided for the use of NYIT students, faculty and staff as approved, in support of programs of the College.

Generally, computing systems and equipment are used carefully and appropriately. However, abuse of equipment or systems that causes disruption of users' productivity, and the integrity of their data and programs, may be subject to discipline or prosecution under College policies, and local, state, or federal laws.

**Purpose**
The purpose of this Code is to define responsible technology usage, particularly for new users who may not be aware of the potential impact of their actions.

**Computer Ethics Policy Statement**
Computers, telecommunications, and information in electronic form create a need for ethical models. Information owners, both individual and institutional, must make a conscious and explicit effort to state and enforce their expectations of ethical behavior. Information users have an obligation to recognize the information owner's rights in order to protect and preserve their own rights to use that information.

Computer based information, recognized as a primary educational and research asset, should be protected from unauthorized modification, destruction, disruption, or disclosure - whether accidental or intentional. The use of these systems is a privilege, not a right, and may be revoked at any time.

**STATEMENT OF RESPONSIBILITIES**

**College Responsibilities**
The College assumes the responsibility to ensure the integrity of its computing systems, workstations, and facilities. Since no system is absolutely secure, however, usage will be monitored to ensure that irresponsible users cannot affect the performance and integrity of other accounts and other users' information or the systems themselves.
**User Responsibilities**
Each user is solely responsible for the usage incurred through his/her account/workstation. Individuals, who intentionally abuse accounts and privileges, degrade system performance, misappropriate resources, or interfere in any way with the operation of the technology, are subject to penalties. If you ever discover what may be a security lapse in our systems, please report your concerns to the Office of Information Technology at once;

**Privacy Statement**
Each user is assigned one or more confidential passwords intended to restrict access to files and systems, including e-mail. However, students and employees should have no expectation of privacy of documents stored on computer systems or in messages sent across the network. The College has the absolute and unconditional right to investigate, review and monitor these materials including, but not limited to: eradication of computer viruses; data access, backup and restoration; hardware and software inventory procedures, including scans for unlicensed software installations; installations, maintenance, updates and repair; investigations relating to compliance with College policies, including the College’s technology policies, and investigation of criminal, unlawful, or unauthorized activities as directed by local, state or federal authorities, or by the senior management of the College.

**Standards for Computer Usage**

Access and use of College computing systems and services is defined below. It applies equally to all users of College owned and operated information systems and equipment.

1. Any access prohibited by state or federal law is unauthorized.
2. Any access or use in support of activities that are prohibited by state or federal law is unauthorized.
3. Individuals who willfully cause loss to authorized account holders by unauthorized access or use shall be held financially responsible for the cost of restoring that user's data, programs, and account balance.

Violators who are members of the College community will be subject to disciplinary action under College regulations applying to their respective status within the College. All violators will be subject to prosecution under any local, state, or federal laws that apply.

**Computer Abuse**
The following are examples of computer abuse (this list is illustrative and not meant to be all-inclusive):

1. Unauthorized use of account and/or password, including but not limited to, ineligibility.
2. Individual accounts cannot be transferred to or used by another person.
3. Attempting to gain access to privileged areas or to accounts that do not belong to you.
4. Frivolous, disturbing, or otherwise inconsiderate conduct including extensive use of workstations, playing games, sending nuisance messages, wasteful or unauthorized use of College supported facilities.
5. Possession or use of programs capable of fraudulently simulating system responses; modification of or possession of systems control information, especially that which reflects program state, status, or accounting; attempts to modify or crash the system.
6. Any violation of the NYIT Student or Employee Code of Conduct which involves technology resources.
7. Use of College resources for non-College related commercial purposes is strictly prohibited. This includes, but is not limited to, development of programs, data processing or computations for non-College-related commercial use, and preparation and/or presentation of advertising materials not related to the College;
8. Using College resources to gain unauthorized access to other systems;
9. Attempting to read another person’s e-mail or other protected files;
10. Using equipment to send obscene or harassing messages,
11. Copying, storing, displaying or distributing copyrighted materials using College computer systems or networks without the express permission of the copyright owner, except as otherwise allowed by copyright law, is strictly prohibited;
12. Using technology for any unethical, illegal or criminal purposes;

Computing Facilities Access and Use Policies
Access to computer facilities by any individual may be restricted or denied for, but not limited to, the following reasons:

- Unauthorized changes to computing facility hardware or software, including but not limited to: disconnecting/reconnecting or reconfiguring hardware; theft; removing, changing, or reconfiguring files on drives; damaging laboratory hardware or software.
- Failure to observe policies, procedures, and protocol, including but not limited to: refusing to leave the laboratory promptly at closing time; refusing to respond to, or responding inappropriately to requests made by facility staff (i.e., a request to move to another machine, to limit output pages to the printer, etc.), in the normal course of carrying out their job responsibilities; using threatening or abusive language or behavior directed at anyone in the facility.
- Attempts to bypass security measures, such as access permissions to files, or obtaining permissions or account attributes with or without authorization.

Violations of this code, including the above lists, may lead to any of the following disciplinary measures:

- Any employee found to be in violation of any of the terms of these policies will be subject to suspension of your access and disciplinary action, up to and including suspension or termination of employment and, if warranted, referral to the appropriate law enforcement agency.
- Violators who are members of the College community will be subject to disciplinary action under College regulations applying to their respective status within the College.
All violators will be subject to prosecution under any local, state, or federal laws that apply

- Termination of a program or online session. NYIT may log off an irresponsible user. Similarly, a harmful job running under the operating system may be cancelled without notice.
- Inactivation of an account-ID.
- Reduction of allocations or restrictions of account privileges.