**Acceptable Use of College Computer and Network Systems by Employees**

**Introduction**
Information Technology Services (ITS) publishes this policy guiding the acceptable use of college computer and network systems in order to inform all staff and faculty of the college of their rights and responsibilities. This is not intended to impose restrictions that are counter to the Canisius traditions of openness, trust, and integrity. Rather, we seek to avoid harm to the College and its employees from illegal or damaging actions by individuals.

**Scope**
This policy applies to staff, faculty, contractors, consultants, and other workers at Canisius College, including all personnel affiliated with third parties. This policy applies to all College-owned or College-leased equipment.

**Acceptable Use**
Canisius College computer and network systems are intended for use in College-related research, instruction, learning, enrichment, and administrative activities. Internet access and all Canisius electronic communication systems, such as e-mail and voice mail, are made available to College Personnel only to carry out their activities on behalf of the College. The College expects faculty, staff, and students to use electronic resources in a lawful and responsible manner consistent with the College’s mission of education, research, and service. Any personal use of these services by College employees shall not interfere with their official responsibilities and shall not violate any College practice or policy.

Users are expected to adhere to reasonable and necessary security habits when using College resources. These habits include:

- Keeping account information, including passwords, confidential;
- Logging out of computers or using a password-protected screensaver when leaving the office;
- Running College-provided antivirus and antispyware software;
- Installing operating system updates when prompted;
- Using caution when opening email attachments and other unexpected data; and
- Adhering to the standards of outside resources accessed from the Canisius network;

**Privacy and Personal Use**
Since the College’s communication systems are the property of the College, all communications are subject to review by appropriate and authorized College Personnel at any time. Data may be retained in backup systems, even after its apparent deletion.

College Personnel should be aware that personal privacy in their use of the College’s communication systems or information sent to or from, or stored in, the College’s communication systems cannot be guaranteed in the event of legal or disciplinary proceedings.

If it appears that the integrity, security, or functionality of the College’s network and computer resources are at risk, Canisius College reserves the right to take any necessary action to investigate and remediate the problem. This action may include monitoring network activity or viewing user-generated files. In such cases, a written report of the findings will be forwarded to the appropriate College officials.

In order to assure continuity for academic and administrative departments, similar procedures may be used after an employee is separated from the College or no longer able to perform required duties.

Employees are responsible for exercising good judgment regarding the personal use of College computing resources. If there is any uncertainty regarding personal use of network or Internet resources, employees should consult with their supervisor or manager. At no time should a College resource be used in a way that is at odds with the employee handbooks published by the Human Resources department.
Unacceptable Use
Under no circumstances shall an employee of Canisius College:

- Engage in any illegal activity using College equipment;
- Engage in any activity contrary to College policy using College equipment;
- Introduce malicious software into the campus computer network;
- Reveal account information or allow the use of College computer resources by people outside of the Canisius community;
- Attempt to breach, disrupt, eavesdrop on, or otherwise tamper with network communication;
- Access a system or resource using another user’s account information;
- Use College equipment or network resources to violate intellectual property laws;
- Use Canisius equipment or network resources for personal commercial or for-profit activities; or
- Use Canisius equipment or network resources for viewing or exchanging pornography.

Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.