I. POLICY & SCOPE

This is the SUNY College at Old Westbury policy on College-provided access to electronic information and services, computing facilities, and networks. This policy applies to all persons accessing or using College Technology Resources. This includes students, faculty and staff, authorized guests, and all persons authorized for access or use privileges by the College, hereafter referred to as Users.

Users of College Technology Resources must comply with federal and state laws, College rules and policies, and the terms of applicable contracts including software licenses. 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 jurisdictions and the rules and policies of those other systems and networks. Questions as to how the various laws, rules and resolutions may apply to a particular use of College Technology Resources should be forwarded to the College's Chief Information Officer. Legal questions should be forwarded to the College's Assistant to the President for Administration.

II. PURPOSE

Access to information technology is essential to the College's mission of providing College educational services of the highest quality. The pursuit and achievement of the mission of education, research, and service require that the privilege of the use of computing systems and software, internal and external data networks, as well as access to the Internet, be made available to all in the College community. The preservation of that privilege for the full community requires that each faculty member, staff member, student, and other authorized User comply with institutional and external standards for appropriate use, whether on campus or from remote locations.

III. RESPONSIBILITIES

All College *Users* are responsible for ascertaining what authorizations are necessary and for obtaining them from the Chief Information Officer before using College Technology Resources. Users are also responsible for any activity originating from their accounts which they can reasonably be expected to control. Accounts and passwords may not, under any circumstances, be used by persons other than those to whom they have been assigned by the account administrator. In cases when unauthorized use of accounts or College Technology Resources is detected or suspected, the account owner should change the password and report the incident.

The College's *Chief Information Officer (CIO*) is responsible for providing College Technology Resources and information technology services to the campus. The CIO or designee may prevent, based on security or legitimate business concerns, in whole or in part, any User from accessing or using the Internet or College systems at any time, without notice.

The College's *Information Security Officer (ISO)* is responsible for overseeing and coordinating the implementation of College policies governing security and privacy on Internet and Email-related College matters. Users should consult with the ISO if there are questions regarding the Internet, College systems and Email security related matters. Absent an authorized ISO position, a College-appointed committee or the CIO may serve in this role.

IV. DEFINITIONS

College Technology Resources – (1) College owned, operated, leased or contracted computing, networking, Email, telephone and information resources, whether they are individually controlled, shared, standalone or networked; (2) information maintained in any form and in any medium within College Technology Resources, and (3) College voice and data networks, telephone systems, telecommunications infrastructure, communications systems and services, and physical facilities, including all hardware (desktop computers, laptops, portable handheld computing devices, personal data assistants (PDAs), "smartphones", etc.), software, applications, databases, and storage media. Additionally, all creation, processing, communication, distribution, storage, and disposal of information by any combination of College Technology Resources and non-College technology resources are covered by this policy.

Incidental Personal Use – minimal or occasional use of College Technology Resources by Users which does not result in any measurable cost or distraction to the College and benefits the College by allowing personnel to avoid needless inconvenience. Under no circumstances may incidental personal use involve violations of the law, interfere with the fulfillment of an employee's College responsibilities, or adversely impact or conflict with activities supporting the mission of the College.

User Account – an established relationship between a User and a computer, network or information service. Use of the College's computer systems and network requires that a User Account be issued by the College. Every computer User Account issued by the College is the responsibility of the person in whose name it is issued. College recognized clubs and student organizations may be issued a User account. Faculty advisors shall designate a particular person(s) authorized to act on behalf of the club or organization. This person(s) is responsible for all activity on the account and will be subject to College disciplinary procedures for misuse. The following will be considered theft of services, and subject to penalties described in the *Enforcement* section of this policy.

- Acquiring a Username in another person's name;
- Using a Username without the explicit permission of the owner and of the Computing Services Department;
- Allowing one's Username to be used by another person without explicit permission of the Computing Services Department; and
- Using former system and access privileges after association with College has ended.

V. PROCEDURES

Security & Privacy Concerns – The College employs various measures to protect the security of its computing resources and its User's accounts. Users should be aware, however, that the College cannot guarantee security and confidentiality. Users should therefore engage in "safe computing" practices by establishing appropriate access restrictions for their accounts, guarding their passwords and changing them regularly and avoiding web sites that have a reputation for being problematic as sources of malware.

Users should also be aware that their uses of College Technology Resources are not private vis-à-vis the College. The College always retains ownership of College Technology Resources. Such ownership provides the College with an inherent right of access. While the College does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of the College's Technology Resources require the backup and caching of data and communications, the logging of activity, the monitoring of

general usage patterns and other such activities that are necessary for the provision of service. The university may also specifically monitor or inspect the activity and accounts of individual Users of College Technology Resources, including individual login sessions and the content of individual communications, without notice, when:

- The User has voluntarily made them accessible to the public, as by posting to a web page;
- It reasonably appears necessary to do so to protect the integrity, security, or functionality of College Technology Resources or other computing resources or to protect the College from liability;
- There is reasonable cause to believe that the User has violated or is violating this policy or any other law or policy;
- An account appears to be engaged in unusual or unusually excessive activity; and
- Accessing the account is otherwise required or permitted by law, including but not limited to freedom of information laws, laws governing the conduct of parties engaged in or anticipating litigation, and laws governing criminal investigations.

Users shall respect the privacy of others. Users shall not intentionally view information of other Users, modify or obtain copies of other Users' files, access or attempt to access other Users' email, or modify other Users' passwords without their permission. College computers and networks are designed to protect User privacy; Users shall not attempt to circumvent these protections.

Restrictions & Prohibitions – The College's Technology Resources are, by nature, finite. All members of the College community must recognize that certain uses of College Technology Resources may be limited for reasons related to the capacity or security of the College's information technology systems, or as required for fulfilling the College's mission. Although there is no set bandwidth, disk space, CPU time, or other limit applicable to all uses of College Technology Resources, the College may require Users of those resources to limit or refrain from specific uses if, in the opinion of the CIO, such use interferes with the efficient operations of the system.

Users shall not use College Technology Resources to excess. Excessive use of College Technology Resources by a particular User, or for a particular activity, reduces the amount of resource available to satisfy the needs of other Users. Excessive use may degrade or jeopardize system functionality, and can result in significant costs to the College. Some examples of excess use may include writing a program or script, using an Internet bot to perform a repetitive task such as attempting to register for a class or purchasing concert tickets online, or keeping your computer logged into Internet radio/video and other streaming media services.

Users are prohibited from using College Technology Resources for personal commercial purposes or for personal financial or other gain. Further limits may be imposed upon personal use in accordance with normal supervisory procedures concerning the use of College equipment.

Users shall not develop or use procedures to alter or avoid the accounting and monitoring of the use of College Technology Resources. For example, Users may not utilize facilities anonymously or by means of an alias, and may not send messages, mail, or print files that do not show the correct Username of the User performing the operation.

Users shall not circumvent or attempt to circumvent security mechanisms or the intent of a system. Users must not use College Technology Resources to gain unauthorized access to remote computers or to impair or damage the operations of computers or networks, terminals or peripherals. This includes blocking communication lines, intercepting or sniffing communications, and running, installing or sharing virus programs. Deliberate attempts to circumvent data protection or other security measures are not allowed.

Users are also expected to refrain from deliberately wasteful practices such as printing unnecessarily large documents, performing endless unnecessary computations, or unnecessarily holding public computers for long periods of time when others are waiting for the same resources.

Users shall not tamper with network services and wiring or extend them beyond the area of their intended use. This applies to all network wiring, hardware and in-room jacks. Users shall not use the College's network to provide Internet access to anyone outside of the College community for any purpose other than those that are in direct support of the academic mission of the College.

Users must use College Technology Resources consistent with local, state and federal laws, including copyright, patent infringement and trademarks, and College policy. Examples of improper and inconsistent use of College Technology Resources include but are not limited to:

- Forwarding appeals soliciting donations to individuals or charities unless approved by a Vice President or Department Head;
- Distributing communications that promote religious, political or personal preferences and activities;
- Sending or forwarding messages containing libelous, defamatory, offensive, sexist, racist or obscene remarks;
- Forging or attempting to forge messages, or disguise identity;
- Utilizing a personal Email account (i.e. AOL, Yahoo!, Gmail, Hotmail, etc.) to conduct College-related matters;
- Downloading, using or distributing illegally obtained media (e.g. software, music, movies); and
- Uploading, downloading, distributing or possessing pornography.

Group/Mass Communications – Many academic and administrative entities on campus are interested in using Email and other digital communication services, such as text messaging, to send important *but unsolicited messages* to large segments of the College community: for example, to all students, all faculty, all staff, or to some combination of these large segments. To moderate the use of sending College-wide digital messages, the College will employ its Rave Alert Notification System to reach the College community on an "opt-in" basis. Mass communications should be used sparingly.

If a faculty member, staff or student desires to send an Email message to multiple parties at the same time for group announcements or news, an Email distribution list can be created within the Rave System.

- Distribution lists and groups within the College Email system will be moderated and monitored by the Information Security Officer (ISO) for proper usage; and
- If a distribution list or group becomes inactive for a period of six months, it will be removed from the College Email system.

Mass digital communications can also be utilized when a College emergency or an urgent need-to-know matter warrants their use. If a College-wide digital message is deemed appropriate and time-critical by the Office of the President, University Police, or the Office of Institutional Advancement, the message should be sent to Office of Institutional Advancement for distribution to the intended parties.

Appropriate content topics include, but are not limited to:

- Urgent security (physical and electronic) matters;
- Natural disaster alerts;
- Significant campus-wide policy changes; and
- Time-critical administrative announcement.

Enforcement: Users who violate this policy may be denied access to College Technology Resources and may be subject to progressive disciplinary action up to possible expulsion or dismissal. Alleged violations will be handled through the College disciplinary procedures applicable to the User. The College may suspend, block or restrict access to an account, independent of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of College or other computing resources or to protect the university from liability. The College may also refer suspected violations of applicable law to appropriate law enforcement agencies.

When the Department of Computing Services becomes aware of a possible violation, an investigation will be initiated in conjunction with the College's ISO and relevant campus offices. Users are expected to cooperate fully in such investigations when requested.

To prevent further unauthorized activity during the course of such an investigation, Computing Services may suspend access to all computing facilities for the User(s) involved in the violation.

VI. REFERENCES

For additional guidance related to this policy please refer to:

- New York State Laws and Notices http://www.its.ny.gov/tables/technologypolicyindex.htm
- New York State Information Technology Policy IT Best Practice Guideline: Acceptable Use of Information Technology (IT) Resources

VII. REVIEW & APPROVAL

This policy was prepared by the Division of Business & Finance and reviewed by the College's Chief Information Officer, the Assistant to the President for Administration, the Assistant to the President for Advancement and the Vice President and CFO prior to approval by the President.

This policy supersedes previously issued College Policies B-03 "Email Procedures" and C-01 "Internet Security Policy".