4-5002 Information Technology Acceptable Use

(1) Purpose. The purpose of this Regulation is to establish and promote the ethical, legal, and secure use of computing and electronic communications for New College of Florida.

(2) Scope. New College acquires, develops, and maintains software, computers, computer systems, and networks for College-related purposes as part of its infrastructure. The College's computing resources and infrastructure are made available to users in support of the College's instructional, research, community service missions, its administrative functions, its student and campus life activities and to promote the free exchange of ideas among members of the College community and between the College community and the wider local, national, and international communities. This regulation governs the use of New College computing resources and infrastructure and applies to all users of the College's computing resources and infrastructure, whether or not affiliated with the College, and also to all uses of those resources, whether from on campus or from remote locations. Users of these resources and infrastructure are responsible for reading and understanding this regulation.

(3) Rights & Responsibilities. The College is committed to intellectual and academic freedom, the diversity of values and perspectives inherent in an academic institution, and to applying those freedoms to the use of its computing resources and infrastructure. However, as with any other College-furnished resource, the use of its computing resources and infrastructure is subject to the normal requirements of legal and ethical behavior within the College Community. Thus, the legitimate use of these resources does not extend to whatever is technically possible. Although some limitations may be built into computer operating systems, software, or networks, those limitations are not the sole restrictions on what is permissible. Users must abide by all applicable restrictions, whether or not built into the operating systems, software, or networks and whether or not they are capable of being circumvented by technical means.

(4) Basic Requirements. All users must comply with all applicable local, state, federal and foreign laws, all generally applicable College rules, policies, procedures and all applicable contracts and licenses. These include, but are not limited to, laws on libel, privacy, copyright, trademark, obscenity, Sexual Harassment Policy, and child pornography; the Florida Computer Crimes Act (Chapter 815, Florida Statutes), the Florida Security of Communications Statute (Chapter 934, Florida Statutes), the Electronic Communications Privacy Act (18 U.S.C. §§ 2510 et seq.), and the Computer Fraud and Abuse Act (18 U.S.C. §1030 et seq.) [which prohibit unauthorized access to computers or networks, or disruption of others' use thereof]; the College Student Code of Conduct and all applicable software licenses. Users who interact with others in different states or countries should also be aware that they may also be subject to the laws of those other states or countries, as well as the rules and policies applicable to other systems or networks.

(5) Restrictions on Use. Users may use only those computing resources which they are authorized to use, and use them only in the manner and to the extent authorized. Users must respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected. The ability to access computing resources, at the College or elsewhere, does not necessarily imply authorization to do so. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before using College computing resources.

(6) User Responsibilities

(a) Basic Responsibility. Users are responsible for any activity originating from their accounts, personal computers, or devices which are attached to the College's network to which they can reasonably be expected to control. Users are responsible for performing basic preventative measures with personal equipment which is attached at any time to the College's network, including running a personal firewall and performing regular virus and spyware scans. The College may periodically probe any computers or devices attached to its network for evidence of such infections, and temporarily suspend/limit connection when found.

(b) Use of Accounts and Passwords. Accounts and passwords may not, under any circumstances, be used by persons other than those to whom they have been assigned by Information Technology. In cases when a user detects or suspects unauthorized use of accounts or resources, the user must change the password and report the incident to Information Technology.

(c) Capacity Limitations. Users should respect the finite capacity of the College's computing resources and infrastructure, and avoid interfering unreasonably with the activity of other users. Although there is no set bandwidth, disk space, CPU time, or other limit applicable to all users of College computing resources, the College may require users of those resources to limit or refrain from specific uses if, in the opinion of Information Technology, such use interferes with the efficient operations of the system.

(d) Activities that Impact Operation of Resources. The College may establish limits on bandwidth, disk space, usage times or other aspects of usage of its computing resources and infrastructure, with which users must comply. Additionally, users may be required to refrain from certain specific activities which adversely impact the operation of the College's computing resources and infrastructure.

(e) Personal Use of Resources. Users must refrain from using the College's computing resources for any personal use that would consume a significant portion of those resources, or interfere with the College's operations or the performance of the individual user's assignments or other responsibilities to the College.

(f) Representation of College. Users may not represent or imply that they speak on behalf of the College without proper authorization to do so. Affiliation with the College does not, by itself, imply authorization to speak on behalf of the institution. Use of the College's trademarks or logos without appropriate authorization in accordance with College regulations is not permitted.

(7) Security and Privacy

(a) Protection of Privacy. The College is committed to protecting the privacy and integrity of computer data and records belonging to the College, individual users, and commercial providers. The College employs a variety of means to protect the security of its computing resources and infrastructure. Users should be aware, however, that the College cannot guarantee such security. Users should therefore engage in responsible computing practices by establishing access

restrictions for their accounts where appropriate, guarding passwords, and changing passwords regularly.

(b) Monitoring Use. Users do not own accounts on College computers, but are granted the privilege of the use of their accounts. Use of the network does not alter the ownership of data stored on the network. Users should also be aware that their use of the College's computing resources and infrastructure is not completely private. While the College does not routinely monitor individual usage of its computing resources or infrastructure, the normal operation and maintenance of those resources requires the backup and caching of data and communications, logging of activity, monitoring general usage patterns, and other such activities. The College may also specifically monitor the activity and accounts of individual users of its computing resources, including individual login sessions and communications, without notice, under the following circumstances:

1. The user has voluntarily made them accessible to the public, as by posting to a Listserv or Web page.

2. When it reasonably appears necessary to do so to protect the integrity, security, or functionality of the College's computing resources or to protect the College from liability.

3. When there is reasonable cause to believe that the user has or is violating this regulation.

4. When an account appears engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns.

5. It is otherwise required or permitted by law. Any such individual monitoring other than that authorized by the user must be authorized in advance by the Provost in consultation with the General Counsel.

(c) Disclosure of Results of Monitoring. The College may, in its discretion, disclose the results of any such individual or general monitoring, including the contents and records of individual communications, to appropriate College or law enforcement personnel, subject to the Family and Educational Rights and Privacy Act (20 U.S.C. §1232(6) and other applicable laws.

(d) Expectation of Privacy. Subject to the exceptions set out above, users have reason to expect the same level of privacy in personal files on the College's computers (e.g., files in a user's home directory) as users have in any other space assigned to them by the College (e.g., a locker or an office).

(e) Policies of Other Network Operators. Other organizations operating computing and network facilities that are reachable via the College network may have their own policies governing the use of those resources. When accessing remote resources from College facilities, users are responsible for obeying both the policies set forth in this document and the policies of the other organizations.

(8) Enforcement. Users who violate this policy may be denied access to the College's computing resources and infrastructure, and may be subject to other disciplinary action or penalties both within and outside the College. Violations will normally be handled through the usual disciplinary

procedures applicable to the particular user (i.e. faculty, administrator, staff or student). However, the College may temporarily suspend or block access to the College's computing resources or infrastructure prior to the initiation or completion of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of the College's or other computing resources.

Authority: Article IX, Sec. 7, Fla. Constitution; Fla. Board of Governors Regulations 1.001 and 3.0075

History: Adopted 03-05-11; Revised 03-02-17 (technical amendment)