Computer and Network Use Policy

I. Introduction and Applicability

Stetson University College of Law 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, and 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 acceptable use policy governs the use of these Stetson University College of Law computing resources and infrastructure. As a user of these resources and infrastructure, you are responsible for reading and understanding this document. This policy 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 remote locations.

The College of Law is committed to intellectual and academic freedom 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.

II. Basic Requirements

All users must:

- Comply with all applicable local, state, federal and foreign laws, all generally applicable College rules and policies, and all applicable contracts and licenses.
  These include, for example, the laws on libel, privacy, copyright, trademark, obscenity, and child pornography; the Florida Computer Crimes Act (Fl. Stat. ch. 815), the Florida Security of Communications Statute (F. Stat. Ch.934), 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 "hacking", "cracking" and similar activities]; the Code of Student Professional Responsibility; and all applicable software licenses (e.g., restriction on academic LEXIS or Westlaw accounts being used as a research tool in the course of employment outside the law school). Users who interact with others in different states or countries should 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.

- Use only those computing resources that they are authorized to use, and use them only in the manner and to the extent authorized. 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 determining and obtaining whatever authorizations may be necessary before proceeding. Accounts and passwords should not be shared or used by persons other than those to whom they have been assigned by the College.

- Respect the finite capacity of the College's computing resources and infrastructure, and avoid interfering unreasonably with the activity of other users.

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.

- 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 job or other responsibilities to the College.

- Refrain from stating or implying 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 is not permitted.

III. Security and Privacy

The College of Law is also committed to protecting the privacy and integrity of computer data and records belonging to the College of Law, 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.
Users do not own accounts on College of Law 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, when (a) the user has voluntarily made them accessible to the public, as by posting to a Listserv or Web page; (b) 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; (c) when there is reasonable cause to believe that the user has or is violating this policy; (d) when an account appears engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns; or (e) 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 Associate Dean for Academic Affairs.

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.

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

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

IV. 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 of Law. Violations will normally be handled through the usual disciplinary procedures applicable to the particular user (i.e. faculty, administrator, staff or student) concerned. 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.

V. Questions Regarding this Policy and Designation of Agent for Notification of Infringement

If you have any questions regarding the Stetson University College of Law Computer Use Policy, or concerns regarding a possible violation of this Policy, please contact the Associate Dean for Academic Affairs. Additionally, in accordance with the Online Copyright Infringement Liability Limitation Act (17 U.S.C. 512), the Director of Information Services is designated as the College's agent for the receipt of any notices concerning any alleged copyright infringements occurring by reason of material being stored, transmitted, routed, or connected through the College's computing resources or infrastructure. For further information regarding the Act or copyright law in general, please refer to the U.S. Copyright Office homepage http://www.copyright.gov/. Notices of any alleged infringements may be sent to:

Office of the Dean
Stetson University College of Law
1401 61st Street South
Gulfport, FL 33707

Phone: 727 562-7809
Email: lawdean@law.stetson.edu

Administrative Revisions, August 20, 2015