Appendix B

USE OF TECHNOLOGY AND THE INTERNET

This policy applies to all “Technical Resources” including those owned or leased by Albany Law School, used on or accessed from Law School premises, or used on Law School business. Such Technical Resources include but are not limited to computers, the communications network, computer accounts, web pages, network access, central computing and telecommunications facilities, and related services. This policy also applies to all activities using any Law School-paid accounts, subscriptions, or other technical services, such as Internet and World Wide Web access, voice mail, and e-mail, whether or not the activities are conducted from Law School premises.

Users of these resources are responsible for reading, understanding, and complying with this policy.

Users of Technical Resources should understand and appreciate the nature of the information created and stored there. Because they seem informal, e-mail messages are sometimes offhand, like a conversation, and not as carefully thought out as a letter or memorandum. Like any other document, an e-mail message or other computer information can later be used to indicate what a user knew or felt. Users should keep this in mind when creating e-mail messages and other documents. Even after an e-mail message, document or image is deleted or a computer or web session is closed, data may still be recoverable and may even remain on the system. All users are responsible for the content of all text, audio, or images that they place or send over Technical Resources. Users may access only files or programs, whether computerized or not, that they have permission to access. Violations of any guidelines in this policy may result in disciplinary action.

In addition, Albany Law School may advise appropriate legal officials of any illegal violations.

Section 1: Authorized Users

Technical Resources are to be accessed and used only by persons who are authorized to use them. A person who does not have a user access code (e.g. password, login id, logon id, etc.) is not an authorized user and is prohibited from using Technical Resources that require user access code authorization. These policies apply to all user groups, including students, faculty, staff, graduates, volunteers and guests.

Section 2: Acceptable Uses

2.1 Access to and use of Technical Resources is a privilege granted to currently enrolled Law School students, faculty, and staff. Technical Resources are provided for the benefit of Albany Law School, its students, faculty, and staff. Limited access to Technical Resources may also be provided to graduates, volunteers and guests. These resources are provided for use in the pursuit of education and Law School business and are to be reviewed, monitored, and used only in those pursuits, except as otherwise provided in this policy. Employees are only permitted to use Technical Resources for occasional, non-
work purposes with permission from their direct supervisor.

2.2 A person having limited authority to use Technical Resources may use them only to the extent of their authority to use them. Limited authority means that: (a) a user is authorized only to access specific data, files, and/or programs, and/or (b) persons having authorized access to specific data, files, or programs must limit the tasks they perform with the data, files, or programs (e.g. a person who is authorized only to view data, files, or programs is not permitted to alter, modify, destroy, or delete them).

Section 3: Unacceptable Uses

3.1 Technical Resources should not be used by employees for personal gain or commercial purposes. Incidental personal use may be permitted with knowledge and consent of the employee's supervisor. No user may engage in solicitation for any non-Law School business or activities using Technical Resources. Faculty use of Technical Resources for non-Albany Law School business should comport to the standards for outside employment outlined in the Faculty Handbook “Terms of Employment Applicable Only to Faculty”. The only other exceptions are found in sections 3.12-3.15 below.

3.2 Albany Law School employees should not conduct Albany Law School business using non-Albany Law School e-mail accounts unless it is impossible to do otherwise.

3.3 Use of Technical Resources must not interfere with the user's productivity, the productivity of other users, or the operation of Albany Law School's Technical Resources. Running or installing on the Law School's Technical Resources, or giving another, a program that could result in degradation of system integrity or stability or in the eventual damage to data is prohibited. This section does not apply to use of programs or utilities to purposely delete unneeded data that the user is authorized to delete.

3.4 Unauthorized review, duplication, dissemination, removal, installation, damage or alteration of files, passwords, computer systems or programs, or other property of the Law School, or improper use of information obtained by unauthorized means, is prohibited.

3.5 Employees may not play games on Albany Law School's computers and other Technical Resources unless such games are primarily designed for an instructional purpose related to their educational or work duties.

3.6 Users shall not attach any computer networking equipment (including, but not limited to, hubs, switches, routers and servers) to the Albany Law School network nor operate any wireless access points on Law School grounds without consent of and coordination with Information Technology Services and/or the Administrative Services Office. No users, except Information Technology Services, may connect port scanning or packet sniffing devices to the Albany Law School network. Use of the 2.4GHz and 5GHz frequencies on
Law School grounds is prohibited except with consent and coordination with Information Technology Services and/or the Administrative Services Office.

3.7 Users should not send e-mail or other communications that either mask the user’s identity or indicate that they were sent by someone else. Users should never access any Technical Resources using another user’s password. Similarly, users should only access the libraries, files, data, programs, and directories that are related to their education/work duties. Nothing in the paragraph will prohibit Information Technology Services from using another user’s password when needed or prohibit a supervisor from using passwords of a subordinate themselves or authorizing another to use the password of a subordinate.

3.8 Sending, saving, or viewing obscene or offensive material on or through Technical Resources is prohibited. Messages stored and/or transmitted by computer, voice, mail, e-mail, or telephone systems must not contain content that may reasonably be considered offensive to any member of the Law School Community. Offensive material includes, but is not limited to, sexual comments, jokes or images, racial slurs, gender-specific comments, or any comments, jokes or images that would offend someone on the basis of his or her race, color, creed, sex, age, national origin or ancestry, physical or mental disability, veteran status, marital status, sexual orientation, or any other category protected by applicable federal, state, or local laws. This policy does not pertain to material and messages directly associated with a faculty member’s academic pursuits or those directly associated with a Law School investigation of violations of Albany Law School policy.

3.9 Storing, transmitting or printing any of the following types of electronic communications on Technical Resources is also prohibited: material that infringes upon the rights of another person; material or behaviors that violate Albany Law School’s Guidelines for Appropriate Conduct or other Law School policies; or material that may injure someone else and/or lead to a lawsuit or criminal charges.

3.10 Violations of this policy or violation of Law School policies in the course of using Technical Resources may result in an immediate loss of computing privileges and may also result in the referral of the matter to the Vice President for Enrollment, Management and Student Affairs, the Dean, or other appropriate authority.

3.11 Albany Law School does not consider conduct in violation of this policy to be within the course and scope of one’s educational endeavors or employment or the direct consequence of the discharge of one's duties. Accordingly, to the extent permitted by law, Albany Law School reserves the right not to provide a defense or pay damages assessed against students or employees for conduct in violation of this policy.

3.12 Use of e-mail accounts for commercial purposes (e.g. advertising for bar review courses, advertising for eating and/or drinking establishments, etc.) is prohibited. Please contact Administrative Services for clarification if needed.
3.13 Except where specifically allowed in this policy, use of e-mail for sale or solicitation of personal goods and services is prohibited. Please contact Administrative Services for clarification if needed. Posting of personal goods for sale by Law School faculty, staff and students is permitted on the Albany Law School Classifieds system. Browse to classifieds.albanylaw.edu for more information. Posting of "sitter" services is permitted by faculty, staff and students using the Albany Law School sitters lists. See intra.albanylaw.edu/sitters for more information.

3.14 Use of e-mail for housing or apartment leases or rentals is prohibited. Please contact the Housing Office for information on posting housing notices using our centralized housing database system.

3.15 Charitable solicitations via e-mail other than those conducted for the United Way, or those conducted on behalf of Albany Law School, must be precleared by the Associate Dean of Academic Affairs. Approved solicitations should begin with the declaration: "This message has been cleared by the Associate Dean of Academic Affairs in compliance with Computer Use Policy 3.15."

3.16 Frivolous mass e-mails to public mailing groups (such as the “students” or “employees" mail distribution lists) are prohibited.

Section 4: Access to Information

All messages, data files and programs stored in or transmitted via Albany Law School's Technical Resources are Law School property, and should not be considered private or confidential. Users should keep in mind that when they are using Albany Law School's Technical Resources they are creating Law School records using a Law School asset. Albany Law School respects the individual privacy of its students, faculty and staff. However, that privacy does not extend to an employee's work-related conduct or to the use of Technical Resources covered by this policy. Users have no right to privacy as to any information or file transmitted through or stored on Technical Resources.

Albany Law School reserves the right to monitor, access and disclose all messages, data files and programs sent over or stored in/on its Technical Resources. Use of Albany Law School’s Technical Resources constitutes consent to all such monitoring, accessing and disclosure.

Information subject to the attorney-client and/or attorney work product privileges stored in/on Albany Law School computer facilities should not be commingled with non-privileged information. Failure to exercise discretion and judgment with respect to this provision may waive privilege or destroy the expectation of confidentiality.

Section 5: Security of Information

Although users may have passwords to access computer, voice mail, and e-mail systems, these Technical Resources belong to Albany Law School, are to be accessible at all times by Albany
Law School, and are subject to inspections by Albany Law School with or without notice. Albany Law School may override any applicable passwords or codes to inspect, investigate, or search files and messages belonging to a member of the Law School Community. All passwords must be made available to Information Technology Services or a supervisor upon request. Users outside Information Technology Services should not provide a password to other users or to anyone outside Albany Law School and should never access any Technical Resources using someone else's password except that employees may do so with the authorization of their supervisor.

In order to facilitate Albany Law School’s access to information on Technical Resources, users may not encrypt or encode any voice mail or e-mail communication or any other files or data stored or exchanged on Law School systems without the express prior written permission from Information Technology Services. As part of this approval, Information Technology Services and the appropriate Department Supervisor will indicate a procedure for users to deposit any password, encryption key or code, or software with Information Technology Services or the Supervisor so that the encrypted or encoded information can be accessed in a user's absence.

Section 6: Copyrighted Materials

Users should not copy or distribute copyrighted material (e.g., software, database files, documentation, articles, graphic files, music and downloaded information) through Technical Resources or by any other means unless they have confirmed in advance from appropriate sources that they have the right to copy or distribute the material. The United States Copyright Office provides basic information about copyright online at http://www.copyright.gov. Failure to observe a copyright may result in disciplinary action by Albany Law School as well as legal action by the copyright owner. Albany Law School's rules and procedures regarding claims of online copyright infringement are stipulated in the Albany Law School Digital Millennium Copyright Act Compliance Policy.

Section 7: Confidential Information

All employees should safeguard Albany Law School's confidential information, as well as that of students and others, from disclosure. Do not access new voice mail or e-mail messages with others present. Messages, files or other computer data containing confidential information should not be left unsecured and easily accessible while you are away from your work area. Employees should not leave passwords to Technical Resources where they can be easily found by unauthorized persons. Where employees are allowed to generate their own passwords, they should not create passwords that can be easily guessed by others.

E-mail messages containing confidential information should include the following statement, in all capital letters, at the top of the message: CONFIDENTIAL: UNAUTHORIZED USE OR DISCLOSURE IS STRICTLY PROHIBITED.
Section 8: Software

If users want to install software on Law School computers, they must contact Information Technology Services and request to have the software installed. Users are prohibited from installing any software on any Technical Resource without the express prior written permission from Information Technology Services.

Involving Information Technology Services ensures that Albany Law School can manage the software on Law School systems, prevent the introduction of computer viruses, and meet its obligations under any applicable software licenses and copyright laws. Computer software is protected from unauthorized copying and use by federal and state law; unauthorized copying or use of computer software exposes Albany Law School and the individual to substantial fines and exposes the individual to imprisonment. Therefore, users may not load personal software onto Albany Law School’s computer system and may not copy software from Albany Law School for personal use. Exceptions may only be made for properly licensed software designed to interface or synchronize with personal productivity devices, such as pda’s or portable data storage devices.

Section 9: Albany Law School Web Sites

Albany Law School makes web services available to support and promote its institutional mission. It is expected that individuals placing information on these servers will abide by all applicable Law School policies and all laws governing the use of the Internet. Users utilizing the Law School’s web services must adhere to the provisions of this policy as well as the Albany Law School Web Policy.