Virginia Tech Carilion School of Medicine (VTCSOM)

Policy: **Computer Use and Electronic Communication**
Subject: **Information Technology**
Administrator: **D. Womack & B. Brindle**
Rev.: **3**
Original date: **11/7/2013**
Revision dates: **10/28/2015, 12/8/2016**

1 Purpose

The use of e-mail has been designated as the primary source of communication between administration and students at VTCSOM. Students are informed of this policy during orientation. Students are expected to check their Carilion Clinic e-mail accounts regularly (daily is recommended) and are responsible for any information disseminated by way of e-mail. In addition to the Carilion Clinic email address, students will be given a Virginia Tech email address. Students are responsible to check their VT email accounts regularly; it is recommended that they forward their VT email to their Carilion Clinic account. Carilion TSG and VTCSOM IT staff are available to assist students in linking email accounts to their mobile devices.

VTCSOM seeks to maximize productivity and minimize misuse of computers by establishment and enforcement of policies and procedures governing the use of computers, peripherals, mobile devices and associated systems. This policy is applicable to all students of, and visitors to, VTCSOM.

2 Policy

Computing resources and network access are provided to support VTCSOM's goals of teaching and learning. Computing resources include but are not limited to administrative computing system, student computers, laptops, server resources and peripherals.

All use of VTCSOM computing and network resources must be in accordance with current federal, state, and school regulations. Willful misuse of any computing resource may result in termination of access privileges, disciplinary action, or civil and criminal penalties.

System users should remember that VTCSOM computers are maintained to help members of the community in their individual and collective educational pursuits. In addition, all faculty, staff, and students should remember that VTCSOM strongly supports academic freedom in the pursuit of research; system users should remember that holding a computer account at VTCSOM is a privilege, not a right. As such, VTCSOM as well as Carilion's Technical Services Group may take whatever steps it feels appropriate to remedy or prevent activities that, in the School's or Carilion Clinic's judgment, endanger the orderly operation of the VTCSOM networks or systems, and which threaten connections to the Internet and other institutions or networks.

3 Procedures

Users' Rights

VTCSOM does not guarantee the privacy of information displayed on computers and peripherals in public areas. Users should keep in mind that they occasionally need the technical assistance of computing personnel, who might unavoidably see private material while providing such assistance. Technical assistance may need to access a user's desktop system via a remote connection to resolve issues. If it is necessary to suspend a user's account, reasonable attempts will be made to notify the user. The user may seek review of any reprimand concerning the use of computing services through the process outlined in the Violations of the SEPCP and/or Teacher-Learner Compact policy.

User Responsibilities
Users are responsible for adhering to existing VTCSOM, Virginia Tech and Carilion Clinic Policy statements not superseded by this document. Such statements include legal use of software, personal abuse, confidentiality and sexual harassment.

All students will obtain a Carilion Clinic e-mail address. It is the student's responsibility to read the contents of his or her Carilion Clinic e-mail account in a timely fashion and respond when appropriate.

E-mail documents are subject to discovery in legal proceedings to the same extent as a hard copy. Therefore, users should treat each e-mail as they would a hard copy that is not controlled and may never be destroyed. Remember that any message may be forwarded to another person without the author's consent. Careful consideration should be given to content. Content should be appropriate for all addressees.

Computer usage shall not interfere with the ability of others in the vicinity to work or study. Usage that may constitute interference includes the generation of offensive, intimidating, or annoying computer images, text, or sounds.

Users must help maintain the security of the systems by keeping their passwords confidential. The user accepts full responsibility for all activities undertaken using their user ID and password. Passwords must be changed every 90 days.

If the use of a given account causes technical problems, for example, the excessive use of storage space, the user will be notified of the problem by the System Administrator. The user must follow the instructions given to rectify the problem. If this is unsuccessful, they should contact support services for further instructions.

Commercial use of VTCSOM computer equipment is prohibited. Software piracy is also strictly prohibited.

Examples of Misuse
Misuse includes, but is not limited to, the activities in the following list:

- Using a computer account that you are not authorized to use; attempting to monitor or tamper with another user's electronic communications; or reading, copying, changing, or deleting another user's files.
- Copying of proprietary information.

- Using the VTCSOM network to gain unauthorized access to any computer systems, or attempting to circumvent data protection schemes or uncover security loopholes. This includes creating or running programs that are designed to identify security loopholes or decrypt intentionally secure data. This also includes programs contained within an account, or under the ownership of an account, that is designed or associated with security cracking.
- Displaying obscene or sexually harassing images or text on a VTCSOM owned computer or on VTCSOM property.
- Knowingly or carelessly running or installing on any computer system or network, or giving to another user, a program intended to damage or to place excessive load on a computer system or network. This includes, but is not limited to, programs known as computer viruses, Trojan Horses, and worms.
- Violating terms of applicable software licensing agreements or copyright laws.
- Deliberately wasting or overloading computing resources, or in any other way knowingly or carelessly performing an act which will interfere with the normal operation of computers, terminals, peripherals, or networks. This includes, but is not limited to, printing multiple copies of a document or printing out large documents that may be available on line, or that might impact significantly on other users printing resources.
- Using electronic mail to harass others, including sending electronic mail that the sender would reasonably anticipate to be unwelcome.
- Creating mail or electronic distribution lists larger than 10 addressees that send electronic communications to other accounts without prior permission of the receiving individual.
- Posting on electronic bulletin boards or any type of electronic forum information that may be slanderous or defamatory in nature or any materials that violate existing laws or the SEPCP.

Enforcement

It is the duty and responsibility of System Administrators to enforce the VTCSOM computer use policy. Minor infractions of this policy, when likely accidental in nature, such as poorly chosen passwords, overloading systems, excessive disk space consumption, and the like are typically handled in an informal manner by electronic mail or in person discussions. More serious infractions are handled via formal procedures.

Infractions such as sharing accounts or passwords, harassment, or repeated minor infractions as described in, but not limited to, the above policies may result in the temporary or permanent loss or modification of computer access privileges, other disciplinary action as outlined in the Violations of the SEPCP Policy and or notification of proper authorities.

If VTCSOM has evidence of misuse of computing and networking resources through a specific account, VTCSOM will take the following steps to protect the systems, networks, and the user community:

- The suspected accounts will be suspended immediately pending the outcome of any investigation.

- The files and data on the account will be inspected for evidence.

The violation will be reported to the appropriate authorities. VTCSOM policy violations will be reported to the Associate Dean for Student Affairs. Illegal activity will be reported to the police, the FBI, the Secret Service, and/or the Attorney General's Office.

Violators are subject to any and all of the following:

- Loss of computing and networking access
- VTCSOM disciplinary actions (in accordance with applicable policies)
- Civil proceedings
- Criminal prosecution
- Loss of the privilege of using college computers, even if temporary, may prevent a student from completing course assignments and from making normal progress in the course.

This is very likely to have a negative impact on the final course grade. To remove the opportunity for students to avoid consequences associated with the violation of this policy, instructors are not allowed to make accommodation for students' course work.

The Electronic Communications Privacy Act of 1986 (ECPA), protects employers and employees from interception, unauthorized access, and disclosure of electronic communications, and governs monitoring of employee e-mail.

Communications system and e-mail messages are property of VTCSOM and are to be used for business purposes. Personal use of e-mail is permitted but such messages will be treated the same as business related messages, in accordance with the e-mail policies and procedures of Virginia Tech.

VTCSOM disclaims responsibility for the content of e-mail messages. While VTCSOM reserves the right to discipline any user for inappropriate use of its e-mail system, it does not intend to screen messages in advance and cannot be responsible for their content. VTCSOM will not defend or protect any user for defamatory or otherwise wrongful e-mail communications. Transmissions made on the Carilion Clinic and Virginia Tech e-mail systems are not private. The use of a password does not ensure that only the sender and recipient of a message are able to retrieve and read it. E-mail may be monitored and the right to do so is reserved, and VTCSOM has the right to disclose a student's messages retrieved from the e-mail system to a third party without further notice or consent. In addition, information obtained from such monitoring may result in discipline or termination.