DEFINITIONS:

♦ **EVMS** includes
  - Eastern Virginia Medical School (EVMS)
  - Eastern Virginia Medical School Health Services (EVMSHS)
  - Eastern Virginia Medical School Pediatric Faculty Associates (EVMSPFA)

♦ **ITMT** refers to the appropriate member of the Information Technology Management Team comprised of the management representatives of:
  - The EVMSHS Data Processing Department
  - The EVMS Business and Financial Information Systems Center
  - The EVMS Network Information Center
  - The EVMS Data Base Center
  - The EVMS Communications Department
  - The EVMS Library Services

♦ **Information Services Department** refers to the technology department/personnel responsible for the related services.

POLICY:

ELECTRONIC MAIL

The Medical School’s electronic mail system and services are the sole property of the Medical School. The Medical School will make reasonable efforts to maintain the integrity and effective operation of its electronic mail system, but users are advised that those systems should in no way be regarded as a secure medium for the communication of sensitive or confidential information. Because of the nature and technology of electronic communication, the Medical School can assure neither the privacy of an individual user’s use of the Medical School’s electronic mail resources nor the confidentiality of particular messages that may be created, transmitted, received, or stored thereby. Users expressly waive any right of privacy in anything they create, store, send or receive on the computer or through the Internet or any other computer network. By accepting an EVMS e-mail account, users consent to allowing EVMS personnel authorized by the President or Dean/Provost as advised by the Dean’s Information Services Subcommittee, Planning & Management Subcommittee to access and review all email materials users create, store, send or receive on computers or through the campus computer network.

In addition, Virginia law provides that communications of EVMS personnel that are sent by electronic mail may constitute correspondence and, therefore, may be considered public records subject to public inspection or subpoena by the legal system.

SERVICE RESTRICTIONS

Those who use EVMS’ electronic mail services are expected to do so responsibly, that is, to comply with state and federal laws, with this and other policies and procedures of the Medical School, and with normal standards of professional and personal courtesy and conduct. Access to EVMS’ electronic mail services, when provided, is a privilege that may be wholly or partially restricted by the Medical School without prior notice and without the
consent of the e-mail user when required by and consistent with law, when there is substantiated reason to believe that violations of policy or law have taken place, or, in exceptional cases, when required to meet time-dependent, critical operational needs. Such restriction is subject to the approval of the President or the Dean/Provost or his/her designee.

PERMISSIBLE USES OF ELECTRONIC MAIL

- **Authorized Users**

  Only EVMS faculty, staff, residents, and students and other persons who have received permission under the appropriate Medical School authority are authorized users of the EVMS’ electronic mail systems and resources. Users are responsible for safe guarding their passwords for access to the computer system. Individual passwords should not be printed, stored online, or given to others. Users are responsible for all transactions made using their passwords. No user may access the computer system using another user’s password or account. Users may not disguise their identity while using the computer system. Users may be required to change passwords periodically.

- **Purpose of Use**

  The use of any EVMS resources for electronic mail must be related to the Medical School’s business, including academic pursuits. Incidental and occasional personal use of electronic mail may occur when such use does not impinge on work time or generate a direct cost for the Medical School. Any such incidental and occasional use of EVMS electronic mail resources for personal purposes is subject to all of the above provisions of this policy.

PROHIBITED USES OF ELECTRONIC MAIL

- Personal use that creates a direct cost for EVMS is prohibited; e.g., sending personal e-mail message during regular working hours.
- For personal monetary gain or for commercial purposes that are not directly related to EVMS business.
- Sending copies of documents in violation of copyright laws.
- Inclusion of the work of others into electronic mail communications in violation of copyright laws.
- Capture and opening of electronic mail except as required in order for authorized employees to diagnose and correct delivery problems.
- Use of electronic mail to harass or intimidate others or to interfere with the ability of others to conduct EVMS business.
- Use of electronic mail systems for any purpose restricted or prohibited by laws or regulations.
- “Spoofing,” i.e., constructing an electronic mail communication so it appears to be from someone else.
- “Snooping,” i.e., obtaining access to the files or electronic mail of others for the purpose of satisfying idle curiosity, with no substantial EVMS business purpose.
- Attempting unauthorized access to electronic mail or attempting to breach any security measures on any electronic mail system, or attempting to intercept any electronic mail transmissions without proper authorization.
- Purposes that could reasonably be expected to cause, directly or indirectly, excessive strain on any computing facilities, or unwarranted or unsolicited interference with others’ use of e-mail or e-mail systems. Such uses
include, but are not limited to, the use of e-mail services to (i) send or forward e-mail chain letters; (ii) “spam”, that is, to exploit list servers or similar broadcast systems for purposes beyond their intended scope to amplify the widespread distribution of unsolicited e-mail; and (iii) “letter-bomb”, that is, to resend the same e-mail repeatedly to one or more recipients to interfere with the recipient’s use of e-mail.

- Broadcast messages, that is an e-mail sent to all e-mail users except when authorized by the President, Dean/Provost, Vice Presidents, ITMT, and/or the Director of Human Resources.
- Use of electronic mail in a sexually explicit, profane, obscene, x-rated, defamatory or threatening manner.
- Use of e-mail to support a “for-profit” activity.

EVMS ACCESS AND DISCLOSURE

General Provisions

- To the extent permitted by law, the Medical School reserves the right to access and disclose the contents of faculty, employees, residents, students’ and other users’ electronic mail without the consent of the user. EVMS will do so when it believes it has legitimate business needs including, but not limited to, those listed in “Inspection and Disclosure of Communications” below and only after explicit authorization is obtained from the President of the Medical School or his/her designee.
- Faculty, employees, residents, students and other users are advised that EVMS’ electronic mail systems should be treated like a shared filing system with the expectation that communications sent or received may be made available for review by any authorized EVMS official for purposes related to EVMS business.
- Electronic mail of students may constitute “education records” subject to the provisions of the federal statute known as the Family Educational Rights and Privacy Act of 1974 (FERPA). EVMS may access, inspect, and disclose such records under conditions that are set forth in the statute.
- Any user of the EVMS’ electronic mail resources who makes use of any encryption device to restrict or inhibit access to his or her electronic mail must provide access to such encrypted communications when requested to do so under the authority of the Medical School President or Dean/Provost or his/her designee.

Monitoring of Communications

EVMS will not monitor electronic mail as a routine matter but it may do so to the extent permitted by law as the School deems necessary for purposes of maintaining the integrity and effective operation of the School’s electronic mail systems.

Inspection and Disclosure of Communications

EVMS reserves the right to inspect and disclose the contents of electronic mail:

- in the course of an investigation triggered by alleged misconduct or misuse,
- as needed to protect health and safety,
- as needed to prevent interference with the academic mission, or
- as needed to locate substantive information required for EVMS business that is not more readily available by some other means.
EVMS will inspect and disclose the contents of electronic mail when such action is necessary to respond to legal processes and to fulfill EVMS’ obligations to third parties.

Limitations on Disclosure and Use of Information Obtained by Means of Access or Monitoring.

• The contents of EVMS electronic mail communications may be disclosed without permission of the user. EVMS will attempt to refrain from disclosure of particular communications if disclosure appears likely to create personal embarrassment, unless such disclosure is required to serve a business purpose or satisfy a legal obligation.

Special Procedures to Approve Access to, Disclosure of, or Use of Electronic Mail Communications.

• Individuals needing to access the electronic mail communications of others, to use information gained from such access, and/or to disclose information from such access and who do not have the prior consent of the user must obtain approval in advance of such activity from the Medical School President or Dean/Provost or his/her designee.

POLICY VIOLATIONS

Appropriate disciplinary action will be taken, up to and including dismissal, against individuals found to have engaged in a prohibited use of EVMS’ electronic mail resources. Illegal acts involving EVMS’ computing resources may also subject users to prosecution by state and federal authorities.

MANAGEMENT OF ELECTRONIC MAIL SYSTEM

Users should review their messages every week and delete those that are not needed. E-mail accounts will be deleted when a user is no longer affiliated with EVMS. Accounts will be deactivated for the infringement of any written or implied policy or any violation of state or federal laws. Accounts that remain unused for periods longer than six months will be deleted unless specific arrangements have been made with the email system administrator.