Privacy of Email, Voice Mail, and Electronic Files
Endorsed by University Faculty Council on May 3, 2006

The University of Richmond intends to provide secure and reliable email and voice mail services for authorized users and uses. Electronic mail and voice mail resources are deployed and maintained by Information Services to support the University’s work of teaching, scholarship, research, administration, and public service.

Information Services monitors and collects data related to the University’s systems and networks as necessary to manage the campus network traffic and to ensure that resources are available for academic, scholarly, and administrative uses. Designated Information Services personnel, such as email system administrators, have special privileges necessary for the implementation and maintenance of the University’s systems and networks. The number of Information Services staff with system administrator privileges for any given system is limited to the number required for smooth operation, cross training, and adequate coverage.

The University respects the privacy of electronic communications in the same way that it respects the privacy of paper correspondence and telephone conversations. Therefore, the University does not routinely monitor or access the content of electronic communications, computer files, or voice mail whether stored on university equipment or in transit on the University network. However, monitoring or access may be necessary under certain circumstances. This policy outlines the legal or administrative circumstances under which access and/or monitoring may occur.

Conditions Under which Email May be Monitored and Accessed
Email mailboxes and stored files are considered private to the account holder and all members of the University are to treat them as such; however the University may inspect, monitor or disclose the contents under the circumstances defined below under the headings of (1) System Administration, (2) Legal Compliance, (3) Emergency Situations, and (4) Other Compelling Circumstances.

1. System Administration

When managing email and file systems, network administrators primarily deal with system logs and email headers. Information Services personnel may not intentionally access the content of email or stored files without the permission of the account holder unless there is a situation that threatens the actual operation of the system. Occasionally, however, because of the way the systems identify and handle problems, Information Services personnel cannot avoid observing the contents of email and other files. These personnel shall peruse these emails and/or stored files as little as possible in order to perform the necessary task. If Information Services staff must observe content, they shall treat the information or content with strict confidentiality and notify the account holder of the incident, except in the case where it is evidence for violations of the law or written University policy.
2. Legal Compliance

The University complies with all valid court orders or other orders with which the University must comply by law. These orders may include preservation, inspection, monitoring, and/or disclosure of email and/or stored files.

The appropriate University official and the account holder shall be notified of these actions, unless the order obligates non-disclosure. For faculty accounts the appropriate University official is the Provost; for staff accounts the appropriate University official is the Associate Vice President of Human Resources; for student accounts the appropriate University official is the Registrar.

3. Emergency Situations

The University may access electronic files or email when access or disclosure is needed to prevent the likelihood of imminent significant harm to persons or property. Even though the situation is deemed an emergency, authorization shall still be sought from the appropriate official. Depending on the emergency and circumstances, notification may not occur until after the situation is resolved. For faculty accounts the appropriate University official is the Provost; for staff accounts the appropriate University official is the Associate Vice President of Human Resources; for student accounts the appropriate University official is the Registrar. Notification of the actions taken shall be given to the account holder.

4. Other Compelling Circumstances

a. The Vice President for Information Services will respond to requests from University Counsel and the University Auditor to preserve information necessary for pending or anticipated litigation or investigations. Only on rare occasions would any of the preserved information be reviewed by Counsel or the Auditor without the permission of the account holder.

b. An appropriate University official with notification of University Counsel may request preservation of email and/or stored files in the event of substantial reason to believe that violations of law or written University policy have occurred. For faculty accounts the appropriate University official is the Provost; for staff accounts the appropriate University official is the Associate Vice President of Human Resources; for student accounts the appropriate University official is the Registrar.

c. In the circumstance when access to stored files or email is necessary to conduct time critical University business and the employee is no longer working at the University or cannot be contacted, an appropriate University official may authorize access to an employee’s email account or electronic files. For faculty accounts the appropriate University official is the Provost; for staff accounts the appropriate University official is the Associate Vice President of Human Resources; for student accounts the appropriate University official is the Registrar.
Resources. This access of stored files or email shall be reported to active employees once they are able to be contacted.

**Notification and Record Keeping**
Information Services shall keep a record of all incidents which require the observation of email content. Observing only email system logs or email headers will not require an entry in this record. Entries shall include the email account id, the date, the IS staff member’s name, and a brief explanation. An annual report summarizing the number and type of such incidents shall be published on the Information Services web site.

**Preservation of Email**
Users of the University’s electronic mail system should be aware that, even though the sender and recipient have discarded their copies of a particular email, back-up copies of discarded email exist for a while, and can be retrieved if necessary. Systems are routinely "backed up" to protect system reliability and integrity, and to prevent potential loss of data. The back-up process results in the copying of data onto storage media that may be retained for periods of time and in locations unknown to the originator or recipient of the email. As a rule, backup tapes of the email system are kept for approximately 30 days. Non-standard system backup tapes may be kept longer.

**No Guarantee of Confidentiality**
Information Services staff follow sound professional practices in providing for the security of the email, data, application programs, and system programs under their control. However, in today’s environment professional practices and protections are not infallible and the security and confidentiality of our systems and data cannot be guaranteed. In addition, the recipient of an email message may forward it to persons who were not intended to see it. Users, therefore, should exercise extreme caution in using email to communicate confidential or sensitive matters.