UNIVERSITY OF RICHMOND

Policy Manual

Policy #:	IRM-4008	**Policy Title:**	Access to Electronic Files Policy
Effective:	02/04/2021	**Responsible Office:**	Information Services
Date Approved:	02/04/2021	**Approval:**	Vice President for Information Services and Chief Information Officer
Replaces Policy Dated:	05/04/2006	**Responsible University Official:**	Vice President for Information Services and Chief Information Officer

PURPOSE:

The University of Richmond 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.

SCOPE:

This policy applies to faculty, staff, and student storage of email, voice mail, and data files maintained in University approved information systems.

INDEX:

POLICY STATEMENT:

IRM-4008.1 – Definitions

User – Any individual, including but not limited to faculty, student, staff, contractors, and visitors who has access and uses University information resources, systems, or data.

IRM-4008.2 – Policy Statement

The University of Richmond owns and provides email, voice, storage, and other electronic services to authorized users to facilitate the University's business and academic mission. These electronic resources are deployed and maintained by Information Services to support the University's work of teaching, scholarship, research, administration, and public service. Incidental and occasional personal use of email and other electronic resources is allowed; however, the University may access such content as described in this policy.

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 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 reliable operation, cross training, and adequate support coverage.

Conditions Under which Email May be Monitored and Accessed

While efforts are made to ensure reasonable expectations of privacy to users' email and electronic files, the University may inspect, monitor, or disclose the contents under the following circumstances:

1. **System Administration** When managing email and file systems, system administrators primarily deal with system logs, application files, 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 may not 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 access user 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 University Counsel and the account holder shall be notified of these actions, unless the order obligates non-disclosure.

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 in consultation with the Senior Associate Vice President for Human Resources or their designee. For faculty accounts the appropriate University official is the Dean of the faculty member; for staff accounts the appropriate University official is the Vice President of the staff's division; for student accounts the appropriate University official is the Registrar. Notification of the actions taken shall be given to the account holder; but depending on the emergency and circumstances, notification may not occur until after the situation is resolved. In the event the Dean or Vice President is not readily available to provide approval, the requestor may defer to the Executive Vice President/Provost for faculty or the Executive Vice President/Chief Operating Officer for staff.

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. When directed, the preserved information may 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 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 Dean of the faculty member; for staff accounts the appropriate University official is the Vice President of the staff's division. In the event the Dean or Vice President is not readily available to provide approval, the requestor may defer to the Executive Vice President/Provost or the Executive Vice President/Chief Operating Officer for staff. This access of stored files or email shall be reported to active employees once they are able to be contacted.

Notification and Record Maintenance – 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.

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 as well as 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.

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.

IRM-4008.3 – Applicable Regulations and Accreditation Standards

A. Red Flags Rule of the Fair and Accurate Credit Transaction Act of 2003 (FACT Act), Public Law 108-159, Section 114
B. Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
C. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191
D. Payment Card Industry Data Security Standard (PCI DSS)
E. SACSCOC *Principles of Accreditation* 10.6 (Distance and Correspondence Education)

RELATED POLICIES:

A. Information Security Policy
B. Acceptable Use Policy
C. Data Security Policy

POLICY BACKGROUND:

Initial policy created May 4, 2006

Revision history added May 18, 2010

Added Deans and VPs as approvers for user files access; EVPs as alternates. Reviewed by IT Governance Committee and President's Cabinet prior to approval. Dec 18, 2020

Revised version approved by Vice President for Information Services and Chief Information Officer Feb 4, 2021

POLICY CONTACTS:

Vice President for Information Services and Chief Information Officer
Director of Information Security
Assistant Vice President for Systems and Networks
Assistant Vice President for Telecommunications, Media Support, User Services, and Academic Computing Services