PURPOSE: To provide guidelines concerning access to and disclosure of electronic email messages sent or received by employees who use the electronic mail system and on the proper use of the electronic mail system generally. Users are reminded that all usage of KSU’s information technology resources, including electronic mail, is subject to all University policies including the information technology appropriate usage policy.

POLICY:
The University encourages the use of electronic mail and respects the privacy of users. It does not wish to inspect or monitor electronic mail routinely or to be the arbiter of its contents. Nonetheless, electronic mail and data stored in the University’s electronic systems are the property of the University. University management may access e-mail accounts for any reason, including:

1. Troubleshooting hardware and software problems
2. Preventing unauthorized access and system misuse
3. Retrieving business related information*
4. Investigating reports of violation of University policy or local, state, or federal law*
5. Complying with legal requests for information*
6. Rerouting or disposing of undeliverable mail

* Note: IT will need approval from the Division Vice President, Legal Consul or appropriate designee to access specific mail and data for these purposes. The extent of the access will be limited to what is reasonably necessary to acquire the information.

Archiving electronic mail is strongly encouraged.

Only Public Relations and other cabinet designated KSU personnel can send electronic mail addressed to the entire campus (Staff, Faculty and Students). Any electronic mail that is to be sent to the entire campus must first be approved by the Vice President of the Division of the sender prior to being sent to Public Relations. Please contact KSU Public Relations for further details on this policy. Any email sent to a specific group (Staff or Faculty or Students), but not the entire campus must be approved by the head of the...
Division. The electronic mail and other information systems are not to be used in a way that may be disruptive, offensive to others, harmful to morale, or would result in a breach of confidential information.

There is to be no display or transmission of sexually explicit images, messages, or cartoons, or any transmission nor use of the e-mail communications that contain ethnic slurs, racial epithets, or anything that may be construed as harassment or disparagement of others based on their race, national origin, sex, age, disability, or religious beliefs.

There should be no expectation of privacy or confidentiality for documents and messages stored on University-owned equipment. Users of e-mail systems should be aware that, in addition to being subject to authorized access and open records laws, electronic mail in its present form cannot be guaranteed secure and is, therefore, vulnerable to unauthorized access and modification by third parties.

Users of e-mail services should be aware that even though the sender and recipient have discarded their copies of an e-mail record, there most likely are back-up copies of such electronic mail that can be retrieved.

University e-mail services may, subject to the foregoing, be used for incidental personal purposes provided such use does not interfere with University operation of information technologies including electronic mail services, burden the University with incremental costs, or interfere with the user’s employment or other obligations to the University.

Electronic mail constitutes a public record like other documents that are subject to disclosure under the Kentucky Open Records Act or other laws, or as a result of litigation. However, prior to such disclosure, the University evaluates all requests for information submitted by the public for applicability of the provisions of the Act or other laws. In addition, electronic mail constitutes University records subject to all the University’s Retention of Records Policy.
Violations of University policies governing the use of University electronic mail services may result in restriction of access to University information technology resources in addition to any disciplinary action that may be applicable under other University policies, guidelines, or implementing procedures, up to and including dismissal.

**POLICIES RELATING TO ACCESS/SECURITY OF CAMPUS E-MAIL**
The following policies relate to electronic mail access at Kentucky State University. KSU policies on electronic mail will also govern electronic mail entering and leaving the campus of KSU.

1. A user ID and password will control access to the campus e-mail system.  
   Note: IT will assign the user ID.

2. KSU does not permit authorized users of the campus e-mail system to share their user ID’s or passwords.

3. Authorized users of the e-mail system are fully responsible for activity performed by their user ID.

4. Faculty or Staff requesting access to the campus e-mail system must complete a “Request for Network Access” form and forward to their Department Head. IT will base authorization for these user ID’s by information supplied on the access form.

5. Each Department Head may delegate responsibilities for authority. They must notify Information Technology of any delegation of authority.

6. Information Technology will administer all authorized access and security for the campus e-mail system.
7. Kentucky State University does not permit authorized users of the campus e-mail system to use the e-mail system except as explicitly stated on their “Request for Network Access” form.

8. Unauthorized use of the e-mail system by an individual not in accord with the mission of Kentucky State University represents a breach of security.

9. Information Technology has the authority to terminate any user’s e-mail access if a breach of security occurs or if security is in question.

10. If an authorized user becomes aware of a security breach involving his or her user ID, it is the responsibility of that user to immediately notify their Department Head and Information Technology of the security breach.

When an authorized employee terminates employment with the University his or her operator ID will be disabled or deleted. The supervisor of the organizational unit for which the terminating employee works most notify Information Technology and IT will disable the users ID on the employee’s last date of employment with KSU or IT will disable account based on the KSU check out list.

1. E-mail access may be suspended or voided if any unauthorized use of the University e-mail systems occur. This may include, but is not limited to, any unauthorized use of any user ID and password.

   Any employee who becomes aware of a breach of security should contact his or her Department Head, or the delegated representative, or IT.

2. IT will suspend all access for the authorized user in question pending a review and analysis of the security breach.

Questions regarding this policy should be directed to the Information Technology Help Desk.