I. **Purpose**

Electronic mail (email) has become a preferred means of communication both internally and externally for the Wilkes community.

The purpose of this policy is to clarify the applicability of law and describe the appropriate use of University email, associated responsibilities, concepts of privacy and security, and rights of all Users of Wilkes University email facilities.

The University recognizes that principles of academic freedom and shared governance, freedom of speech, and privacy of information hold important implications for email and email services. The University affords email privacy protections comparable to that which it traditionally affords paper mail and telephone communications. This Policy reflects these firmly-held principles within the context of the University’s legal and other obligations.

II. **Applicability**

This Policy applies to all electronic email systems and services managed for or owned by Wilkes University; all users, and all University email records in the possession of University employees or other users of electronic mail services provided by the University.

The Policy applies only to email in its electronic form and does not apply to printed copies. Electronic mail messages, in either their electronic or printed forms, are subject to records management policies, including provisions of those policies regarding retention and disclosure.

This Policy applies equally to transactional information (such as email headers, summaries, addresses, and addressees) associated with email records as it does to the contents of those records.

III. **Policy**
Electronic mail, like postal mail, is an official means for communicating Wilkes University business. All students, faculty and staff are expected to read, and shall be presumed to have received and read, all email messages sent to their official Wilkes email account.

Policies and regulations that apply to other forms of communications and the use of technology resources also apply to email facilities. In addition, the following specific actions and uses of University email facilities are improper:

- Any use of email that interferes with University activities and functions or does not respect the image and reputation of Wilkes University.
- Concealment or misrepresentation of names or affiliations in email messages.
- Alteration of source or destination address of email.
- Use of email for commercial or private business purposes that have not been approved by the administration.
- Use of email for organized political activity or political solicitation.
- Use of email to harass or threaten other individuals.

Users whose actions violate this policy or any other University policy or regulation may be subject to revocation or limitation of email privileges as well as other disciplinary actions or may be referred to appropriate external authorities.

The University respects the privacy of its email users. It does not routinely inspect, monitor, or disclose email. Nonetheless, subject to the requirements for authorization, notification, and other conditions specified in this Policy, the University may deny access to its email services and may inspect, monitor, or disclose email: (a) when required by and consistent with law; (b) when there is substantiated reason (reliable evidence indicating that violation of law or of policies probably has occurred) to believe that violations of law or of University policies have taken place; (c) when there are compelling circumstances where failure to act may result in significant bodily harm, significant property loss or damage, loss of significant evidence of one or more violations of law or of University policy, or significant liability to the University or to member of the University community; or (d) under time-dependent, critical operational circumstances where failure to act could seriously hamper the ability of the University to function administratively or to meet its teaching obligations.

Email, whether or not created or stored on University equipment, may constitute a University record subject to disclosure under the Pennsylvania Open Records Laws (Sunshine Act and the Right-to-Know Law), or other laws, or as a result of litigation. However, the University does not automatically comply with all requests for disclosure, but evaluates all such requests against the precise provisions of the Act, other laws concerning disclosure and privacy, or other applicable law.
Destruction of such records is governed by the University's records retention policies.

Email may not be used for communicating confidential information. Common examples of confidential contents included: student grades, personnel records, individual donor gift records, data subject to the Family Educational Rights and Privacy Act (FERPA) and the Gramm Leach Bliley Act (GLBA).

The University considers any message targeted for more than 100 addresses to be a Mass email. Mass emails are subject to the following controls.

(a) The University's central email systems automatically block attempts to email more than 100 addresses in a note.

(b) Execution: Any uses of University equipment to deliver essentially the same note to more than 100 recipients through mechanisms other than appropriate use of distribution lists must be approved by the Director of the Marketing and Communications Department or a University Vice President. Attempts to circumvent this restriction whether from inside or outside can result in loss of access to University information technology, and disciplinary action.

(c) Origin: Mass email requests must originate in department, division, or school administration, not from lower-level units.

(d) Content: Use of mass email is restricted to email from the University which is relevant to official University business, the University's mission, and a significant segment of the campus community. Mass email is considered an appropriate form for communication of an informational item under the following circumstances: Emergency or crisis situations (including closings and delays due to hazardous weather conditions or power outages, the need to provide special assistance to students, etc.); occurrence of crimes that threaten public safety; sudden changes in traffic, campus vehicular access and parking due to emergencies; planned or sudden disruption of significant computer network features; other critical and time-sensitive situations affecting the campus as a whole.

(e) Alternatives: For announcements that do not meet the preceding criteria, such as campus events, advertising, or other promotional activities, a variety of options are available to the University community. These options include announcements via Today @ Wilkes, The Beacon, or appropriate departmental newsletters; mailings, memoranda, and distributed announcements; announcements placed on other University Web pages; posting of events on the "Events Calendar" or departmental calendars; posting to an appropriate distribution list with permission of the list owner; links from an informational email item to a Web site for purposes such as surveys or voting.

The purpose of email is to enhance communication. As such employees will have a signature at the bottom of their email that contains the following:
IV. Responsibilities

The author of any email on the University system assumes the responsibility for assuring that messages do not violate any University policies, regulations, or procedures. Disclaimers of confidentiality included in email do not protect the sender if confidential information is shared or disclosed inappropriately.

Users should regard email communications as non-confidential and think of it as a postcard in that anyone who receives it can read it. For instance, email intended for one person could be widely distributed because of the ease with which recipients can forward it to others. A reply to an email message posted on an electronic bulletin board intended only for the originator of the message may be distributed to all subscribers. Furthermore, even after a user deletes an email record it may persist on backup facilities, and thus be subject to disclosure under the provisions of records management policies. The University cannot routinely protect users against such eventualities.

The University can not protect users from receiving email they may find offensive. Members of the University community, however, are strongly encouraged to use the same personal and professional courtesies and considerations in email as they would in other forms of communication.

Users must obtain approval from the Director of Marketing and Communications or a University Vice President before sending a message to more than one hundred members of the Wilkes University community.

Employee’s emails must contain a signature containing the required elements.

Routing and Communication Process

| Information Technology Advisory Committee |   |

Page 4 of 5 01-2-06
<table>
<thead>
<tr>
<th>Instructional Technology Committee</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative Process Committee</td>
<td></td>
</tr>
<tr>
<td>President’s Cabinet</td>
<td></td>
</tr>
<tr>
<td>Communication of policy:</td>
<td></td>
</tr>
<tr>
<td>IT Webstie</td>
<td></td>
</tr>
<tr>
<td>Updated student technology guide</td>
<td></td>
</tr>
<tr>
<td>Faculty and staff technology guide</td>
<td></td>
</tr>
<tr>
<td>Wilkes Today</td>
<td></td>
</tr>
</tbody>
</table>