Item 3 of the General Policies sections currently states:

University IT resources are for use in conducting authorized University business. Using these resources for personal gain or illegal or obscene activities is prohibited. Although not an inclusive list, examples of such use include theft, fraud, gambling, copyright infringement, sound or video recording piracy, and either viewing or distributing child pornography.

The proposed change is:

University IT resources are for use in conducting authorized University business. Using these resources for personal gain or illegal or obscene activities is prohibited. This prohibition against using IT resources for personal gain does not apply to scholarly activities, including the writing of textbooks or preparation of other teaching materials by faculty members, as recognized in the Statement of Policy on Patents, Copyrights, and Licensing. Consulting and other activities that relate to the faculty member’s professional development and have been approved under the External Activities for Pay Policy are also not included in the prohibition of using IT resources for personal gain. Although not an inclusive list, examples of illegal or obscene use include theft, fraud, gambling, copyright infringement, sound or video recording piracy, and either viewing or distributing child pornography.

Just as minimal personal telephone use is allowed and is sometimes necessary, employees should use the same discretion concerning the University’s IT resources. Therefore, minimal personal use of these resources is permitted by this policy except when such use is excessive or interferes with the performance of the user’s University responsibilities, results in additional incremental cost or burden to the University’s IT resources, or is otherwise in violation of this policy. Further restrictions may be imposed upon personal use by user’s supervisor or in accordance with normal supervisory procedures concerning the use of University equipment.

Item 11 of the Privacy section currently states:

Employee electronic mail may be a public record and may be open to public inspection under the Tennessee Open Records Act. The University also reserves the right to preserve or inspect any information transmitted through or stored in its computers, including e-mail communications and individual login sessions, without notice when:

- There is reasonable cause to believe the user has violated or is violating this policy, any campus guidelines or procedures established to implement this policy, or any other University policies;
- An account appears to be engaged in unusual or unusually excessive activity;
- The user has voluntarily made information accessible to the public such as a Web page;
• It is necessary to do so to protect the integrity, security, or functionality of the University's IT resources or to protect the University from liability; or
• It is otherwise permitted or required by law, such as subpoena or court order.

_The proposed change is:_

While the University recognizes the role of privacy in an institution of higher learning and every attempt will be made to honor that ideal, there should be no expectation of privacy of information stored on or sent through University-owned information systems and communications infrastructure except for certain records relating to students; research; proprietary, trade secret, or patentable material; or certain medical records.

Employees who receive requests under the Tennessee Public Records Act should **not** release documents. All requests should be forwarded to the Public Information Officer who will review the request, contact the General Counsel if needed, and oversee any disclosures.

The University also reserves the right to preserve or inspect any information transmitted through or stored in its computers, including e-mail communications and individual login sessions, without notice when:
• There is reasonable cause to believe the user has violated or is violating this policy, any campus guidelines or procedures established to implement this policy, or any other University policies;
• An account appears to be engaged in unusual or unusually excessive activity;
• The user has voluntarily made information accessible to the public such as a Web page;
• It is necessary to do so to protect the integrity, security, or functionality of the University's IT resources or to protect the University from liability; or
• It is otherwise permitted or required by law, such as subpoena or court order.