Code of Ethics

Information Technology Services Code of Ethics

an Information Technology Services Policy

(Human Resources Policy #44 - last update August 2015)

EAST TENNESSEE STATE UNIVERSITY

SECTION: PPP-44

SUBJECT: Information Technology Services Code of Ethics

Objectives of this Policy

The objectives of this policy are: 1) to articulate the rights and responsibilities of persons using information technology resources owned, leased, or administered by East Tennessee State University (ETSU), 2) to protect the interests of users and ETSU; and 3) to facilitate the efficient operation of ETSU information technology systems.

Definitions

"Information technology resources" or "IT resources" include computers and computer time, data processing or storage functions, computer systems and services, servers, networks, printers and other input/output and connecting devices, and related computer records, programs, software, and documentation.

"Personal or private for-profit use" shall mean a use of ETSU information technology resources which has as a primary objective financial gain of the user. Activities by a student, which are typical of the student job search process, (e.g. use of campus e-mail to contact potential employers or posting of one's resume on ETSU's website) are not to be considered personal or private for-profit uses.

"Public record" means all documents, papers, letters, maps, books, photographs, microfilms, electronic data processing files and output, films, sound recordings, or other material, regardless of physical form or characteristics made or received pursuant to law or ordinance or in connection with the transaction of official business by any governmental agency. (Tennessee Code Annotated, Title 10, Chapter 7, Section 301 (6).)

Supplementary Institutional Policies and Regulations

ETSU is authorized and encouraged to develop additional Institution-specific policies and regulations relating to the use of information technology resources, provided such policies and regulations are consistent with Federal and State law and with this and other policies of the Tennessee Board of Regents. In particular, ETSU may develop policies and regulations regarding installation of non-standard software (including shareware, freeware, or software developed or purchased by the user) onto ETSU IT resources.

Conformance with State Policies

This policy is intended to be fully consistent with the State of Tennessee Internet Acceptable Use Policy and the State of Tennessee Electronic Mail Acceptable Use Policy, as they currently exist or as they may be amended in the future, as well as with any other applicable policies regarding information technology systems which may be promulgated in the future by the State of Tennessee Department of Finance Office of Information Resources (OIR). To the extent that a discrepancy exists between this policy and State policy, State policy shall take precedence.

Applicability

This policy shall apply to all persons and organizations using the information technology facilities and resources owned, leased or administered by ETSU, including all persons employed (either as full-time, part-time or temporary employees or as independent contractors) by ETSU, and to all students enrolled at ETSU. Those provisions contained herein which apply solely to employees and independent contractors are so identified individually. Unless so identified, provisions contained herein apply equally to all persons and organizations covered by this policy.

User Responsibilities

The following lists of user responsibilities are intended to be illustrative, and not exhaustive. Subject to conformance with Federal and State of Tennessee law and with State of Tennessee and Tennessee Board of Regents policies, ETSU is authorized to supplement the user responsibilities contained herein.

Access

1. Users shall obtain proper authorization before using TBR or ETSU information technology resources.
2. Users shall not use TBR or ETSU information technology resources for purposes beyond those for which they are authorized.
3. Users shall not share access privileges (account numbers and passwords) with persons who are not authorized to use them.
4. Users shall not use TBR or ETSU information technology resources in an attempt to access or to actually access computers external to the TBR or ETSU system when that access is not authorized by the computer's owner (no "hacking" allowed).

Respect for Others

1. A user shall not attempt to obstruct usage or deny access to other users.
2. Users shall not transmit or distribute material that would be in violation of existing TBR or ETSU policies or guidelines using ETSU technology resources.
3. Users shall respect the privacy of other users, and specifically shall not read, delete, copy, or modify another user's data, information, files, e-mail or programs (collectively, "electronic files") without the other user's permission. Users should note that there should be no expectation of privacy in electronic files stored on the resident memory of a computer available for general public access, and such files are subject to unannounced deletion.
4. Users shall not intentionally introduce any program or data intended to disrupt normal operations (e.g. a computer "virus" or "worm") into ETSU information technology resources.
5. Forgery or attempted forgery of e-mail messages is prohibited.
6. Sending or attempts to send unsolicited junk mail or chain letters is prohibited.
7. Flooding or attempts to flood a user's mailbox is prohibited.

Respect for State-Owned Property

1. A user shall not intentionally, recklessly, or negligently misuse, damage or vandalize ETSU information technology resources.
2. A user shall not attempt to modify ETSU information technology resources without authorization.
3. A user shall not circumvent or attempt to circumvent normal resource limits, logon procedures, or security regulations.
4. A user shall not use ETSU information technology resources for purposes other than those for which they were intended or authorized.
5. A user shall not use ETSU information technology resources for any private or personal for-profit activity.
6. Except for those not-for-profit business activities which are directly related to an employee's job responsibilities or which are directly related to an organization which is affiliated with ETSU, a user shall not use ETSU information technology resources for any not-for-profit business activities, unless authorized by the President (or his/her designee).
7. Users shall at all times endeavor to use ETSU information technology resources in an efficient and productive manner, and shall specifically avoid excessive game playing, printing excessive copies of documents, files, data, or programs; or attempting to crash or tie-up computer resources.

Additional Responsibilities of Employees and Independent Contractors

1. Employees and Independent Contractors shall not make use of ETSU information technology resources for purposes, which do not conform to the purpose, goals, and mission of ETSU and to the employee's job duties and responsibilities.
2. Employees shall not use ETSU information technology resources for solicitation for religious or political causes.

No Unlawful Uses Permitted

Users shall not engage in unlawful uses of the information technology system resources of the TBR or ETSU. Unlawful activities violate this policy and may also subject persons engaging in these activities to civil and/or criminal penalties. This list of unlawful activities is illustrative and not intended to be exhaustive.

Obscene materials

The distribution and display of obscene materials is prohibited by the laws of Tennessee (see Tenn. Code Ann. § 39-17-902). Obscene materials are defined under Tennessee law (see T.C.A. § 39-17-901(10)) as those materials which:

1. The average person applying contemporary community standards would find that the work, taken as a whole, appeals to the prurient interest;
2. The average person applying contemporary community standards would find that the work depicts or describes, in a patently offensive way, sexual conduct; and
3. The work, taken as a whole, lacks serious literary, artistic, political, or scientific value.

Federal law (18 U.S.C. 2252) prohibits the distribution across state lines of child pornography.

Defamation

Defamation is a civil tort that occurs when one, without privilege, publishes a false and defamatory statement, which damages the reputation of another. ETSU information technology resources should not be used for defamation.

Violation of Copyright

Federal law gives the holder of copyright five exclusive rights, including the right to exclude others from reproducing the copyrighted work. Sanctions for violation of copyright can be very substantial. Beyond the threat of legally imposed sanctions, violation of copyright is an unethical appropriation of the fruits of another's labor.

Pursuant to the Digital Millennium Copyright Act of 1998, the TBR designated agent for receipt of complaints of copyright infringement occurring with the use of ETSU

information technology resources is the Tennessee Board of Regents Assistant Vice Chancellor for Information Technology. ETSU has designated the Chief Information Officer, Information Technology Services as ETSU's campus agent regarding complaints of copyright infringement. After review, the ETSU President will forward complaints received to the TBR Assistant Vice Chancellor for Information Technology.

Gambling

Gambling, including that performed with the aid of the Internet is prohibited under Tennessee state law (see Tenn. Code Ann. §39-17-502).

World Wide Web Home Pages

The principles of use articulated above in Sections 6 and 7 are generally applicable to World Wide Web home pages. For example, use of ETSU information technology resources to post a web page for personal or private for-profit use is prohibited under Section 6.3.5. Illegal content in web pages stored on ETSU ITS resources is prohibited under Section 6.2.2. Obscene content is prohibited under Section 7.1. Incorporation of copyrighted material, without either permission of the copyright holder or under a lawful exemption, is prohibited under Section 7.3.

In addition to the principles of use outlined in Sections 6 and 7, users may not incorporate into web pages or other electronic documents the trademarks or logos of others without express, written permission. Persons who are not employees of ETSU may not make use of ETSU trademarks or logos without express, written permission. The President has designated the Executive Assistant to the President for University Relations the authority to approve a proposed use of ETSU's trademarks and logos by employees on ETSU's web pages.

Advertising

Use of ETSU information technology resources to promote or advertise activities or entities which are not related to ETSU, is prohibited unless such use is consistent with the mission of ETSU and results in substantial benefit to ETSU. The President is authorized to determine whether a given use is consistent with the mission of ETSU and results in substantial benefit to ETSU, consistent with other TBR Policies (in particular, TBR Policy 3:02:02:00). Sale of advertising in web-based versions of ETSU-affiliated student publications is specifically permitted.

ETSU Monitoring and Inspection of Electronic Records

Electronic records sent, received, or stored on computers owned, leased, or administered by ETSU are the property of ETSU. As the property of ETSU, the content of such records, including electronic mail, is subject to inspection by ETSU personnel. While ETSU does not routinely do so, ETSU is able and reserves the right to monitor and /or log all network activity of users without notice, including all email and Internet communications. Users should have no reasonable expectation of privacy in the use of these resources.

Disclosure of Electronic Records

Pursuant to the Tennessee Code Annotated, Title 10, Chapter 7, and subject to exemptions contained therein, electronic files (including email correspondence) which are 1) generated or received by ETSU employees and 2) either owned or controlled by the State or 3) maintained using ETSU ITS resources may be subject to public inspection upon request by a citizen of the State of Tennessee. ETSU personnel receiving such a request for public inspection should refer the request to the Executive Director, University Relations. Institutions may charge reasonable fees for making copies of such records, pursuant to T.C.A. §10-7-506. The charge for copies of printed material at ETSU is $1.00 per page.

While disclosure under T.C.A. Title 10, Chapter 7 applies to employees, disclosure of the electronic records of all users which are maintained using ETSU ITS resources may be made pursuant to a valid subpoena or court order, when otherwise required by federal, state or local law, or when authorized by the President.

Retention of Electronic Records

Electronic records needed to support Institutional functions must be retained, managed, and made accessible in record-keeping or filing systems in accordance with established records disposition authorizations approved by the Public Records Commission and in accordance with TBR Guideline G-070, "Disposal of Records." Each employee of ETSU, with the assistance of his or her supervisor as needed, is responsible for ascertaining the disposition requirements for those electronic records in his or her custody. The system administrator is not responsible for meeting the record retention requirements established under T.C.A. Title 10, Chapter 7, and ETSU, as owner of electronic records stored on ETSU computers, reserves the right to periodically purge electronic records, including email messages. Users who are either required to retain an electronic record, or who otherwise wish to maintain an electronic record should either:

1. Print and store a paper copy of the record in the relevant subject matter file; or
2. Electronically store the record on a storage medium or in an electronic storage location not subject to unannounced deletion.

Violations of this Policy

Reporting Allegations of Violations

Persons who have reason to suspect a violation of this policy, or who have direct knowledge of behavior in violation of this policy should report that allegation of violation to the Director, Human Resources.

Disciplinary Procedures

The Director, Human Resources shall refer allegations of violations of this policy to the appropriate person(s) for disciplinary action. If a student, the policy violation will be referred to the judicial officer of the institution under TBR Policy 3:02:00:01. If an employee, the

policy violation will be referred to the immediate supervisor. If there is a policy violation, which the Director, Human Resources believes rises to the level of a serious violation of this or any other TBR policy; the Director, Human Resources is authorized to temporarily revoke access privileges. In those cases, the revocation of access must be referred to the appropriate disciplinary authority for review and final determination of access privileges. In such cases the authority of the Director, Human Resources carries with it the authorization to make subjective judgments, such as whether material or statements violate TBR policy.

Sanctions

Persons violating this policy are subject to revocation or suspension of access privileges to ETSU ITS resources. Additionally, other penalties, as outlined in TBR Policy, 3:02:00:01, may be imposed upon student users. Sanctions for violation of this policy by employees may extend to termination of employment. Violations of law may be referred for criminal or civil action.

Appeals

Sanctions imposed upon students at a TBR University and imposed at the discretion of the Director, Human Resources may be appealed to the Vice President for Student Affairs. Other sanctions may be appealed under established Institution procedure.

Enforcement of this Policy (Employees)

Procedures and Sanctions

It is reiterated that users' access to ETSU's computing resources is not a right, but a privilege, and is not completely private. While the university does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of the university's computing resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for maintaining network availability and performance.

The university may also specifically monitor the activity and accounts of individual users of ETSU computing resources, including individual login sessions and communications, without notice. The monitoring may occur, but is not limited to, the following instances:

1. The user has voluntarily made them accessible to the public.
2. It reasonably appears necessary to do so to protect the integrity, security, or functionality of the university or to protect ETSU from liability.
3. There is reasonable cause to believe that the user has violated, or is violating, this protocol.
4. An account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns.
5. Upon receipt of a legally served directive of appropriate law enforcement agencies.

Any such monitoring, other than by voluntary disclosure, which is required by law, or necessary to respond to bona fide emergency situations, must be authorized in advance by the Director of Human Resources or the Chief Information Officer, Information Technology Services. In all such cases, the appropriate department or division supervisor will be informed as time and the situation will allow. In all cases, all individuals' privileges and right of privacy are to be preserved to the greatest extent possible.

All users and units have the responsibility to report any discovered unauthorized access attempts or other improper usage of ETSU computers, networks, or other information processing equipment. If you observe, or have reported to you (other than by a law enforcement agency), a security or abuse problem with any ETSU computer or network facilities, including violations of this policy:

1. Take immediate steps as necessary to ensure the safety and well being of information resources. For example, if warranted, your supervisor should be advised so as to have the Office of Human Resources or Information Technology Services to temporarily disable any offending or apparently compromised computer accounts, or to temporarily disconnect or block offending computers from the network.
2. Ensure that the following people are notified: (1) your immediate supervisor (unless that person is the suspected violator), (2) the Director of Human Resources, and/or (3) the Chief Information Officer, Information Technology Services.

Investigation of suspected computer resources abuses involving faculty and staff personnel, other than those initiated by external law enforcement agencies, will be coordinated by the Director of Human Resources. The Chief Information Officer, Information Technology Services, will cause all involved systems resources to be examined for violations outlined in this protocol, the Faculty Handbook, the Student Handbook, and/or the ETSU "Code of Ethics for Computer Resources Use." Activities that appear to be criminal in nature, such as fraud, theft, or child pornography, will be referred to the Department of Public Safety and/or Internal Audit. In examining computer systems or files which may contain patient health care information or student academic records, technical staff personnel and administrators conducting reviews of alleged violations will be guided in their duties by all provisions of privacy and confidentiality as afforded by the Health Insurance Portability and Accountability Act (HIPAA), and the Family Educational Rights and Privacy Act (FERPA). Files, which are identifiable, by patient’s or student names will not be opened or examined, and identities of patients or students will not be disclosed in written reports of infractions nor in discussions about the investigation.

Corrective Procedures

The ETSU procedure for correction of computer resources abuse is a graduated approach to handle violations of this protocol. The approach is based on two premises:

1. The vast majority of users are responsible, and
2. Most offenders, given the opportunity to stop uncivil or disruptive behavior, without having to admit guilt, will do so and will not repeat the offense.

This policy distinguishes between incidents that pose no immediate dangers to persons or to system integrity, and incidents that do. The process described below is designed for cases in which there are no immediate dangers.

First Warning

The Director of Human Resources will send a warning letter to the alleged perpetrator(s) of improper use of ETSU computing resources, harassment, or other uncivil behavior. The letter will have this form:

"Someone using your account did [whatever the offense is]." This is followed by an explanation of why this behavior violates ETSU policy. "Account holders are responsible for the use of their accounts. If you are unaware that your account was being used in this way, it may have been compromised. Your system administrator can help you change your password and re-secure your account. If you are aware, then please make sure that this does not happen again."

This warning ensures that the alleged perpetrators are aware that a policy violation may have occurred and that there was a complaint. It offers them a chance to desist, and/or an opportunity to secure their account against unauthorized use.

This warning is optional, based upon the severity and breadth of the violation(s); however, gross violations may be referred directly to a disciplinary review. The Director of Human Resources may require that the account holder attend a mandatory interview. The Chief Information Officer, Information Technology Services, and/or computer resources personnel may also be asked to attend, to provide technical information pertaining to the particular violation. Access to the user's account may be temporarily suspended by the Director of Human Resources, pending the interview. The user may request that his supervisor and an advocate attend the interview, if desired.

Final Warning/Disciplinary Procedures

If the previous warning stage does not convince the perpetrators to desist, the matter will be turned over to the appropriate supervisory authority (Director, Chair, or Vice President) for disciplinary action. The Director of Human Resources will make available all information or evidence held on the case to the supervisory authority. If it appears from the evidence that any federal or state laws may have been violated, the Director of Human Resources may suspend the account pending the outcome of the university's or law enforcement authorities' investigation.

Temporary Suspension of Individual Privileges

In the event there are reported unauthorized access attempts or other improper usage of ETSU computers, networks, or other information processing equipment which may impose dangers to persons or systems integrity, the Chief Information Officer, Information Technology Services will be authorized to take immediate steps as necessary to ensure the safety and well-being of information resources. For example, offending or apparently

compromised computer accounts may be temporarily disabled, disconnected, or blocked from the network.

Acknowledgment

All current university employees will be required to review the ETSU Code of Ethics for Computer Usage acknowledgment upon login to university computers. Clicking the agree button during login signifies the user understands and will comply with the ETSU Code of Ethics for Computer Usage. All employees will be required to agree at each login.

Use of Computing Resources for Bona Fide Research

Persons engaged in the conduct of bona fide research which involves subject or source materials which may be considered obscene or otherwise prohibited by this protocol will be required to state, in writing, their need to deviate from these prohibitions. A memorandum describing the research project will be submitted with the endorsement of their Chair and Dean, to the Chief Information Officer, Information Technology Services. This memorandum will be filed with Information Technology Services.

Laptops, Personally Owned Desktop or Computers Provided by External Funding

All computers connecting to the ETSU network, regardless of their location or source of funding, are subject to the terms of this protocol and the ETSU Code of Ethics for Computer Usage.

If you have questions or problems implementing any of the above please call or email Information Technology Services at 439-4648 or ITSHelp@etsu.edu.

Approved: Information Technology Governance Council

Reviewed: November 2015

//   // //   // //   // // $(function() { $("#rightColumn").stick_in_parent({ parent: ".float_container" }); }); //