A11.0

SUBJECT: ACCEPTABLE USE POLICY

DATE: February 12, 2018

STANDARD: This document represents the Nashville State Community College's (NSCC) policy for the acceptable use of computers and networks that are made available to faculty, staff, and students. The act of accessing your computer account represents your acceptance of the following policy.

Section 1 Objectives of this Policy

The objectives of this policy include: 1) to articulate the rights and responsibilities of persons using information technology resources owned, leased, or administered by Nashville State Community College (NSCC); 2) to protect the interests of users and NSCC; and 3) to facilitate the efficient operation of NSCC information technology systems.

Section 2 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 NSCC 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) 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. TCA § 10-7-301(6)

Section 3 Supplementary Institutional Policies and Regulations

All supplementary policies and procedures adopted by NSCC will be consistent with Federal and State law and with other policies of the Tennessee Board of Regents.

Section 4 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, and the Tennessee Board of Regents (TBR) Information Technology Resources Policy (1:08:00:00), 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) or the Tennessee Board of Regents (TBR). To the extent that a discrepancy exists between this policy and State or TBR policy, precedence will occur in the following order: State policy, TBR policy, and NSCC policy.

Section 5 Applicability

This policy shall apply to all persons and organizations using the information technology facilities and resources owned, leased or administered by NSCC, including all persons employed (either as full-time, part-time or temporary employees or as independent contractors) by NSCC and all students enrolled at NSCC. 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.

Section 6 User responsibilities

The following lists of user responsibilities are intended to be illustrative, and not exhaustive.

Section 6.1 Access

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

Section 6.2 Respect for others

1) A user shall not attempt to obstruct usage or deny access to other users. This would include but is not limited to use of disk space as well as use of bandwidth.
2) Users shall not transmit or distribute material that would be in violation of existing NSCC policies or guidelines using NSCC information 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. In all circumstances, the fact that a resource is unprotected does not imply permission for an unauthorized person to use it.
4) Users shall not intentionally introduce any program or data intended to disrupt normal operations (e.g. a computer "virus" or "worm") into NSCC 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.
8) Users of computing resources are expected to conduct themselves in a manner that does not constitute a danger to any person's health or safety, interfere with, or harass individuals or institutional activities.
9) Only email messages conveying information concerning official college business are to be broadcast to all or most users of the NSCC email system(s). For purposes of clarity, "Official College Business", means information regarding safety, security, or that which is necessary to maintain the day to day efficient function of the College, specifically:
    a) Administrative messages from the President, Vice Presidents, Deans or Directors.
    b) Announcements of officially recognized faculty/staff committee meetings.
    c) Departmental announcements pertaining to all faculty/staff, i.e. library activities, training/professional development opportunities, network/phone outages, performances, newsletters, events.
    d) Alerts concerning campus facilities and personnel, i.e. alarms, networks, electrical, safety/security (Rave Alerts).
    e) Internal Postings for Human Resources.
    f) Death of an Employee. This will be done only with the family's permission.
    g) Retirement of an employee.
    h) The President's Office may send emails to the entire campus and the Vice Presidents may send emails to their respective divisions directly from their NSCC email accounts as needed for communication. Official College Business information may be forwarded to an email account named campus.announcements@nscc.edu. This email address will be managed by the Human Resources department. Violations of the policy regarding mass distribution email messages and the clarification presented here will be addressed as set forth in Section 14 of the policy. All other provisions in the current policy remain in effect. If you are not sure whether an email that you want distributed campus-wide falls within the definition of "Official College Business" please consult with the Office of Human Resources or the President's Office before you hit "send".
10) The Human Resources department is to be solely responsible for sending email notices regarding deaths, retirements, new hires, and other human resource-related matters to the campus. Any individual or department wishing to make a general announcement about such events must work through the Human Resources department.
11) Use of removable storage media (including but not limited to flash drives, external hard drives, DVD, and CD-ROM) to store confidential or personal identifiable information is strongly discouraged. If required by an employee's job responsibilities, removable storage media should only be used if the media is protected and with written authorization of management. Employees should seek advice on acceptability of removable storage media security from the Computer Services Division.
12) Employees should make every effort to safeguard all removable storage media and laptop computers at all times. Employees should limit the amount of personal information on these devices to that information which is relevant and pertinent to the applicable duties of the employee. See 6.2.11 for additional requirements.
13) Unauthorized peer-to-peer file sharing (of music, movies, etc) and/or copyright infringement is strictly prohibited and subject to civil and criminal penalties.
14) Compliance with the Password Policy is required of all computer and network users.

15) The sending of unencrypted Personally Identifiable Information by end-user messaging technologies (for example, e-mail, instant messaging, chat) is prohibited.
16) Personal web pages of Nashville State students, faculty, and staff do not in any way constitute official school content. The views and opinions expressed in an individual's web pages are strictly those of the author. Comments towards the content of these pages should be directed to the author.

Section 6.3 Respect for State-owned property

1) A user shall not intentionally, recklessly, or negligently misuse, damage or vandalize NSCC information technology resources.
2) A user shall not attempt to modify NSCC 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 NSCC information technology resources for purposes other than those for which they were intended or authorized.
5) A user shall not use NSCC 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 NSCC, a user shall not use NSCC information technology resources for any not-for-profit business activities, unless authorized by the Director of Computer Services Division (or his/her designee).
7) Users shall at all times endeavor to use NSCC 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.
8) Users shall utilize software only in accordance with the applicable license agreement. NSCC licenses the use of most of its computer software from a variety of outside companies. NSCC does not own this software or its related documentation and, unless authorized by the license, does not have the right to reproduce it.

Section 6.4 Additional Responsibilities of Employees and Independent Contractors

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

Section 7 Digital/Electronic Signatures and Transactions

Nashville State Community College must comply with the Tennessee Uniform Electronic Transactions Act (T.C.A. §47-10-101 et seq.) This Act permits the use of electronic signatures and electronic transactions under certain circumstances.

1) In order to be legally enforceable, an electronic signature must meet the following two criteria.

a. An electronic signature must be attributable (or traceable) to a person who has the intent to sign the record or contract with the use of adequate security and authentication measures that are contained in the method of capturing the electronic transaction (e.g., use of personal identification number or personal log-in identification username and password) (T.C.A. §47-10-109) (If Public Key Infrastructure technology ("PKI") is to be used in the creation of the digital signature, contact the Director of Computer Services Division who will contact the TBR Chief Information Officer prior to implementation.)
b. The recipient of the transaction must be able to print or store the electronic record of the transaction at the time of receipt. (T.C.A. §47-10-109)

2) The use of electronic/digital signatures in compliance with state and federal laws is permitted.

Section 8 No unlawful uses permitted

Users shall not engage in unlawful uses of the information technology system resources of NSCC. 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.

Section 8.1 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.

Section 8.2 Defamation

Defamation is a civil tort which occurs when one, without privilege, publishes a false and defamatory statement which damages the reputation of another. Users should be professional and respectful when using electronic media to communicate with others; the use of college resources to libel, slander, or harass any other person is not allowed and could lead to college discipline as well as legal action by those who are the recipient of these actions.

Section 8.3 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 information technology resources is the TBR Chief Information Officer. The TBR agent shall develop and maintain a policy regarding receipt and disposition of complaints of copyright infringement. The Director of Computer Services Division is the NSCC designated agent. Upon receipt of complaints of copyright infringement, the NSCC Director of Computer Services Division shall promptly inform the TBR Chief Information Officer.
The illegal use, downloading, copying, or distribution of materials (i.e. proprietary music, video, software, or database information) via NSCC information technology resources is prohibited.
Section 8.4 Gambling
Gambling, including that performed with the aid of the Internet, is prohibited under Tennessee state law (see Tenn. Code Ann. § 39-17-502).

Section 9 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 NSCC 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 NSCC IT 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 NSCC may not make use of NSCC trademarks or logos without express, written permission. The Director of Creative Services must also approve all proposed use of NSCC trademarks and logos by employees on web pages.

Section 10 Advertising

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

Section 11 NSCC monitoring and inspection of electronic records

Electronic records sent, received, or stored on computers owned, leased, or administered by NSCC is the property of Nashville State Community College. As the property of NSCC, the content of such records, including electronic mail, is subject to inspection by NSCC personnel. While NSCC does not routinely do so, NSCC is able and reserves the right to monitor and / or log all network activity of users without

notice, including all e-mail and Internet communications. Users should have no reasonable expectation of privacy in the use of these resources.

Section 12 Disclosure of electronic records

Pursuant to the Tennessee Code Annotated, Title 10, Chapter 7, and subject to exemptions contained therein, electronic files (including e-mail correspondence) which are 1) generated or received by NSCC employees and 2) either owned or controlled by the State or 3) maintained using NSCC IT resources may be subject to public inspection upon request by a citizen of the State of Tennessee. NSCC personnel receiving such a request for public inspection should refer the request to the Vice President of Finance and Administration or Vice President of Academics (or his/her designee). NSCC may charge reasonable fees for making copies of such records, pursuant to T.C.A. § 10-7-506.
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 NSCC IT resources may be made pursuant to a valid subpoena or court order, when otherwise required by federal, state or local law.

Section 13 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 NSCC, 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 NSCC, as owner of electronic records stored on NSCC computers, reserves the right to periodically purge electronic records, including e-mail 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.

Section 14 Violation of this policy

Section 14.1 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 of Computer Services Division or his/her designee.
It is the responsibility of each direct supervisor to address use by their direct reports of NSCC IT resources (including announcement boards, discussion boards and College’s email system(s)) which is not in compliance with college, TBR, State, and Federal regulations. Supervisors are authorized to take appropriate action as noted below to prevent further misuse of these

systems by their employees. If misuse continues, it is the responsibility of the appropriate Vice President to take further action against both the employee and the supervisor.

Section 14.2 Disciplinary procedures

Allegations of violation of this policy shall be referred by the Director of Computer Services Division to the appropriate person(s) for disciplinary action. If a student, the policy violation will be referred to the Dean of Student Services 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 of Computer Services Division believes rises to the level of a serious violation of this or any other NSCC policy, the Director of Computer Services Division is authorized to temporarily revoke access privileges after consultation with the Vice President of Finance & Administration or the President. In those cases, the revocation of access must be reviewed by the appropriate disciplinary authority for review and final determination of access privileges. In such cases the authorization of the Director of Computer Services Division carries with it the authorization to make subjective judgments, such as whether material or statements violate NSCC Policy.

Section 14.3 Sanctions

Persons violating this policy are subject to revocation or suspension of access privileges to NSCC IT 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.

Section 14.4 Appeals

Sanctions imposed upon students at Nashville State Community College and imposed at the discretion of the Director of Computer Services Division may be appealed to the Dean of Student Services. Other sanctions may be appealed under established Institution procedure.
TBR Source: TBR Board Meeting June 28, 2002; March 30, 2007

Change log

Date	Change	By
2/12/2018	Expanded section 6.2.9 email policy per Dr. McCormick	PAK