NORTHEAST COMMUNITY COLLEGE

ADMINISTRATIVE PROCEDURE NUMBER: AP-3511.1

FOR POLICY NUMBER: BP – 3511

ACCEPTABLE USE PROCEDURES – TECHNOLOGY RESOURCES

1. PROCEDURE SUMMARY STATEMENT

To establish procedures relating to the acceptable use of technology resources including, but not limited to, information, electronic and computing devices and network resources.

2. DEFINITIONS

In this Procedure the following terms shall be defined as follows:

2.1 Systems shall mean and include computers, servers, laptops, mobile devices, facsimiles, copy machines and telephone systems including any software and peripherals required to make the computing equipment function.

2.2 Services shall mean a set of related people, processes and technology provided in support of one or more business functions.

2.3 Networks shall mean and include video, voice and data networks, routers, and storage devices.

2.4 Technology Resources shall mean and include, but are not limited to, information, systems, services, and networks that are administered by the College and for which the College is responsible.

3. PROCEDURE

3.1 Rights and Responsibilities

3.1.1 Accepting a password, operator ID, or other security access code and/or using Northeast Community College technology resources shall constitute an agreement on behalf of the user or other individuals accessing such technology resources to abide and be bound by the provisions of this procedure.

3.1.2 The use of College technology resources are services made available to students, faculty, staff, Board of Governors and other individuals and entities who have an association with the College with proper authorization to further the educational mission of Northeast Community College.

3.1.3 Technology systems can provide access to resources on and off campus, as well as the ability to communicate with other users worldwide. Such open access is a privilege, not a right and requires that individual users act responsibly. Users must respect the rights of other users, respect the integrity of the systems and related physical resources, and observe all relevant laws, regulations, and contractual obligations. Technology systems are college property and are intended for education use and not for personal use.

3.1.4 Northeast Community College supports academic freedom. Users are allowed to use technology resources as necessary to meet educational goals or fulfill work-related responsibilities.

3.1.5 The College technology resources may not be used for transmitting, retrieving or storing any communications of a discriminatory or harassing nature or obscene materials. Harassment of any kind is prohibited. Messages in violation of the College Nondiscrimination policy (BP – 1010) are prohibited.

3.1.6 User files may be subject to search under court order if such files are suspected of containing information that could be used as evidence in a court of law. In addition, system administrators may access user files as required to protect the integrity of computer systems. Student files, as kept on College facilities, are considered educational records as covered by the Family Educational Rights and Privacy Act of 1974 (Title 20, Section 1232(g) of the United States Code, also referred to as the Buckley Amendment). System administrators may access or examine files or accounts if evidence exists that such an intrusion is warranted.

3.1.7 College technology systems are the property of the College and users should not assume electronic communications are private. All users are notified that system security features such as passwords and message delete functions do not take away the ability to archive any message, at that time, for future viewing.

3.1.8 Originators of all web pages using information systems associated with the College shall comply with College policies and are responsible for complying with all federal, state, and local laws and regulations, including copyright laws, obscenity laws, laws relating to libel, slander, and defamation, and laws relating to piracy of software.

3.2 Existing Legal Context

3.2.1 Users may be held accountable for their conduct under any applicable College policies, procedures, or regulations. Complaints alleging misuse of College technology resources will be directed to those responsible for taking appropriate disciplinary action as specified

under the Enforcement section. Misuse of technology resources may result in the loss of access to technology resources and prosecution under applicable statutes. Illegal reproduction of software and associated documentation licensed to the College is protected by U.S. Copyright Law and is subject to civil damages and criminal penalties including fines and imprisonment. All existing laws (federal and state) and College regulations and policies apply, including not only those laws and regulations that are specific to computers and networks, and other technology resources, but also those that may apply generally to personal conduct.

3.2.2 When accessing remote resources from College facilities, users are responsible for obeying both the policies set forth in this document and the policies of the other organizations.

3.2.3 This procedure is effective at all College locations and online, and it represents the minimum requirements that must be in place. Individual areas that have technology resources and networks may have additional controls and security, but they are in addition to this policy. A notice may be posted in computer laboratories or on websites to provide further information in regard to procedures, restrictions or use of facilities that are in effect at that particular location.

3.3 Examples of Misuse

3.3.1 Examples of misuse include, but are not limited to the following:

3.3.1.1 Unauthorized use of another individual's identification or a technology resource account. Examples include obtaining a password for a technology resource account without the consent of the account owner. If you, as an authorized user, give out your account and password to another individual, you may be held accountable for any actions that arise associated with your account.

3.3.1.2 Gaining unauthorized access to any technology resource.

3.3.1.3 Intentionally interfering with the normal operation of technology resources.

3.3.1.4 Intentionally running or installing on any technology resource, a program intended to damage or to place excessive load on a technology resource.

3.3.1.5 Installing or removing software without the permission from the employee responsible for the inventory of the computer.

3.3.1.6 Attempting to circumvent data protection schemes or

uncover security loopholes.

3.3.1.7 Violating terms of applicable software licensing agreements or copyright laws.

3.3.1.8 Deliberately wasting/overloading technology resources.

3.3.1.9 Storing large files on the systems which could compromise system integrity or preclude other users' right of access to disk storage.

3.3.1.10 Masking the identity of a technology resource user to gain anonymity for malicious purposes.

3.3.1.11 Attempting to monitor or tamper with another user's electronic communications.

3.3.1.12 Reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner.

3.3.1.13 Modifying or deleting files in violation of the Records Management Policy (BP3070) or Procedure (AP3070.0). Configuration and setup files will not be changed or removed from College owned systems without authorization from Technology Services.

3.3.1.14 Using computer facilities to interfere with the work of another student, faculty members, or institutional official.

3.3.1.15 Using electronic mail to send abusive, obscene or illegal communications.

3.3.1.16 Using technology resources for non-college consulting, business, or employment.

3.3.1.17 Violating any state or federal law or regulation in connection with use of any technology resource.

3.3.2 Activities will not be considered misuse when authorized in writing by appropriate College officials for security or performance testing, or for approved classroom activities.

3.4 Enforcement

3.4.1 Northeast students discovered in violation of the above will be reported to the Director of Student Conduct.

3.4.2 College staff and faculty discovered in violation of the above will be reported to their supervisor. If violations continue, the staff or faculty

person will be reported through the normal organizational structure.

3.4.3 Violation of any provision of this policy may result in (a) a limitation on a user's access to some or all College systems, (b) the initiation of legal action by the College, including, but not limited to, criminal prosecution under appropriate State and Federal laws, (c) the requirement of the violator to provide restitution for any improper use of service, and (d) disciplinary sanctions, which may include suspension, dismissal or expulsion from a class or the College.

3.5 Disclaimer

3.5.1 College staff responsible for technology resources will make reasonable effort to ensure the integrity of the systems and of the information stored on them. However, users must understand that the College does not take responsibility for the safe storage of non-record or personal files. Users must keep their own copies of any information that is important per the Record Management Policy (BP3070) and Procedures (AP3070.0). Northeast Community College is not responsible for any loss of non-record or personal files from College technology resources, regardless of the cause.

3.5.2 Information posted by users on computer bulletin boards, electronic boards, electronic forums, Web pages, or other publicly accessible sites administered by the College, is subject to review for conformity with legal requirements, including copyright provisions, and with the procedures described in this document. Postings found to be unacceptable will be removed.

4. APPLICABILITY

N/A

ISSUE DATE: 04/26/2017
EFFECTIVE DATE: 04/26/2017
REVISION DATE(S): none
PRIOR POLICY/PROCEDURE NUMBER: AP-3510.0, AP-5250.0
SCHEDULE FOR REVIEW: 2022
DIVISIONS/DEPARTMENT RESPONSIBLE FOR REVIEW & UPDATE: Technology Services
SPONSORING DIVISION/DEPARTMENT: Technology Services
RELATED PROCEDURES/ REFERENCE: AP-3511.0, AP-3511.2
PROCEDURE KEY WORDS: acceptable use; electronic resources; computer; security; technology