ACCEPTABLE USE OF TECHNOLOGICAL RESOURCES

Policy Title: Acceptable Use of Technological Resources

Policy Type: Administrative

Policy Number: 32-01 (2014)

Approval Date: 07/14/2014

Responsible Office: Information Technology Services

Responsible Executive: Vice President for Finance and Administration

Applies to: University Community

POLICY STATEMENT

Norfolk State University (NSU) technological resources are for official use only. Use other than for University business, education, or research is prohibited.

TABLE OF CONTENTS **PAGE NUMBER**

DEFINITIONS

Chain E-mail: An E-mail that is sent to a number of people that requests each recipient to send copies with the same request to other individuals.

Computer Network: Two or more computers that can share information, typically connected by cable, data line, or satellite link.

Intellectual Property: any product of the human intellect that is unique, novel, and unobvious and that fits, but is not limited to, one or more of the following categories: an idea, an invention, an expression of literary creation, a business method, an industrial process, a chemical formula, an issued patent, a copyrighted work, or a legal right inherent in a patent, copyright, trademark, or know-how or trade secret.

Internet: An international network of independent computer systems. The World Wide Web is one of the most recognized means of using the Internet.

Internet Services: include, but are not limited to, electronic mail, file transfer protocol, Telnet, news, and the World Wide Web.

Sensitive System: A system that processes any data of which the compromise with respect to confidentiality, integrity, and/or availability could have a material adverse effect on NSU interests, the conduct of NSU programs, or the privacy to which individuals are entitled (e.g., Colleague Financial and SIS)

Sensitive Information/Data: Any data of which the compromise with respect to confidentiality, integrity, and/or availability could have a material adverse effect on COV interests, the conduct of agency programs, or the privacy to which individuals are entitled.

Examples:

Personally Identifiable Information, including information that describes, locates or indexes anything about an individual including financial transactions, Social Security numbers, medical history, ancestry, religion, political ideology, criminal or employment record and photographs

- Proprietary research data
- Certain confidential proprietary data
- Network diagrams and IP addresses
- Server names and configurations
- Contract cost estimates

Spam: An electronic message is "spam" if: (1) the recipient's personal identity and context are irrelevant because the message is equally applicable to many other potential recipients; and (2) the recipient has not verifiably granted deliberate, explicit, and still-revocable permission for it to be

sent; and (3) the transmission and reception of the message appears to the recipient to give a disproportionate benefit to the sender.

Technological Resources: Technological resources include but are not limited to: computers and terminals, software, printers, networks and equipment, telecommunication equipment and services such as telephones, facsimile machines, modems, basic and long distance calling service, and voicemail; television and radio systems and equipment; computer information systems; and, data files and/or documents managed or maintained by the University which reside on disk, tape or other media. Technology resources also include multimedia equipped classrooms, computer classrooms, computer laboratories, computer offices, and computer furnishings operated or maintained by NSU.

Users: Faculty, staff and students as well as others who have been authorized to use Norfolk State University's technological resources, i.e. contractors, interns, volunteers, etc.

CONTACT(S)

Information Technology Services officially interprets this policy. Finance and Administration is responsible for obtaining approval for any revisions as required by BOV Policy # 01 (2014) https://www.nsu.edu/policy/bov-01.aspx through the appropriate governance structures. Questions regarding this policy should be directed to Information Technology Services (ITS).

STAKEHOLDER(S)

University Faculty & Staff
Students
Information Technology Services

PURPOSE

This policy familiarizes users with the purposes for which technological resources are provided, and the types of activities that are prohibited. The policy also informs users on their responsibilities toward ensuring acceptable use, and, provides other important information pertaining to the administration and operation of technology resources performed by the Information Technology (ITS).

COMPUTER NETWORK ACCOUNTS

Users are responsible for maintaining the privacy and security of their computer network account user IDs and passwords and for the computer information systems accessed through the network. Users are also responsible for the activities carried out under their user accounts. Users are granted access to computing, networks, telecommunications, and electronically stored information

contingent upon their prudent and responsible use. Access is granted to the individual only. Individuals are not authorized to transfer or share access with another.

NO PRIVACY EXPECTATION

As specified by the Commonwealth of Virginia, users should have no expectation of privacy in any message, file, image or data created, sent, retrieved, or received through the use of Norfolk State University's systems and equipment (Commonwealth of Virginia Department of Human Resources Management Policy Number 1.75 is relevant.) Furthermore, electronic communication should never be considered private, confidential, or secure. Once sent, copies of e-mail can be forwarded to other parties and unintended recipients without the sender's knowledge or permission. E-mail should be prepared with the same level of care and discretion as paper-based correspondence. However, users should be aware that the University will make reasonable attempts to maintain the confidentiality and security of electronic communication.

USER RESPONSIBILITIES

Users with email addresses assigned by NSU (e.g. jdoe@nsu.edu) should ensure that emails sent with the NSU Domain Name do not damage or have the potential to damage the good reputation of NSU. Consequently, the University expects users to always act in a professional, lawful, and ethical manner.

When using University technological resources, users must:

1. Use the systems only for approved purposes and in accordance with Commonwealth of Virginia and University policies;

2. Maintain the conditions of security under which they have been granted access;

3. Make every effort to ensure that downloading of network and/or Internet-based material is performed in as safe a manner as possible;

4. Check with Client Services prior to downloading material that may have potential to affect network security and/or integrity (e.g. a virus-infected file);

5. Respect intellectual property rights, including but not limited to applicable software copyright laws;

6. Observe the applicable policies of external networks when they are accessed;

7. Show valid university identification when requested by authorized personnel;

8. Promptly report any policy violations, destruction of data/information or equipment, and other problems to Information Technology Services;

9. Never engage in any of the prohibited activities specified below.

PROHIBITED ACTIVITIES

Within reason, freedom of speech and access to information for business and academic purposes will be honored. Prohibited activities include, but are not limited to:

1. Using University technological resources for personal gain, soliciting or marketing of commercial ventures, or performing other non-job related solicitations;

2. Intentionally accessing, downloading, printing or storing information with sexually explicit content which is prohibited by law (see Code of Virginia §2.1-804 805);

3. Intentionally downloading and/or transmitting fraudulent, threatening, obscene, intimidating, defamatory, harassing, discriminatory, or otherwise unlawful messages or images;

4. Intentionally installing and/or downloading unauthorized or personal computer software/programs and executable files;

5. Uploading, downloading, storing, or transmitting copyrighted materials or proprietary information without proper approval;

6. Uploading, downloading, storing, or transmitting access-restricted University information in violation of University policy or without proper approval;

7. Installing or using proprietary encryption hardware/software;

8. Initiating or forwarding chain e-mail;

9. Intentionally initiating or forwarding SPAM email;

10. Intentionally using anonymizing or disguising technology, to conceal or otherwise suppress the origin of a transmission or message or, one's identity, or using the identity of another person, or an assumed name;

11. Intentionally permitting unauthorized individuals to use University technological resources in any manner;

12. Adding, removing, or modifying NSU owned or administered equipment, data, or documents without specific authorization by the owner or designated administrator;

13. Intentionally downloading video, audio, data, or any other files that cause excessive network and/or computing system traffic or load;

14. Providing information about or lists of NSU users to external organization or individuals without proper authorization or approval;

15. Tampering, defeating or attempting to defeat security systems (locks, surveillance cameras, alarms, firewalls, networks, etc.), attempting or gaining unauthorized access to University information, information technology, facilities, systems and/or other IT-based resources, and/or using proxies, encryption, covert channels or other software and measures to bypass information and physical security controls.

16. Connecting ancillary equipment, (routers, hubs, wireless access points, firewalls, servers, network diagnostic equipment, etc.), to the University's network and systems without obtaining ITS clearance. Clearance requests must be sent to the Information Security Officer via email (security@nsu.edu) and the requestor must fully explain what type of equipment they want to connect and why it is needed. When devices without proper clearance are detected, their network ports are promptly disabled and an investigation is promptly initiated;

17. Knowingly introducing computer viruses, worms, or similar types of programs into computer systems;

18. Denying/attempting to deny or to interfere with University services;

19. Although not strictly prohibited, users must be especially careful when attaching internal or external devices (external disk drive, printers, interface cards, modems, video systems, etc.) to NSU equipment because this can cause internal conflicts as well as damage to systems and might result in service disruptions;

20. Any other activities prohibited by university, state, and federal regulations.

The following additional security precautions apply to University employees, contractors, temporary employees, student workers, external parties, and others accessing University sensitive systems and data:

21. Accessing websites which are not directly related to the conduct of University business while accessing sensitive University system.

22. Installing, using online chat applications, computer games, peer-to-peer file sharing software or other software which is not directly related to the conduct of University business.

23. Installing online storage applications, such as OneDrive, Google Drive, or storing University data on online storage.

    Note: This restriction does not apply to students and faculty using online storage for academic purposes only, i.e. teaching the use of online storage, or sharing class/educational

material not containing sensitive/protected information.

23. Copying or storing, sensitive University data on personal storage, personal computing devices, mobile devices, or any other unapproved media.

24. Transmitting, uploading, downloading, or emailing, sensitive University data to non-University or unapproved systems.

UNIVERSITY MONITORING

ITS specialists frequently monitor network and computer systems access and utilization. This is done for various purposes which include: assessing systems availability and performance; identifying and resolving technical problems; to detect computer viruses, spyware, file-sharing software, etc. and/or to detect prohibited activities; to enforce University administration's directives and/or orders properly issued by law enforcement and legal authorities.

In any investigation of misuse, the University may inspect, without prior notice, the contents of files, voice mail, logs, and any related computer-generated or stored material, such as document output;

Account holder's computer files may be inspected occasionally when assuring system integrity or performing related authorized resource management duties;

WORLDWIDE WEBSITE ACCESS

The Worldwide Web is rich with information that can be of significant benefit when used properly by education and supporting personnel. NSU users accessing the Internet/Worldwide Web must understand:

1. The University is not responsible for material viewed or downloaded by individual users of the Internet. For example, a situation may occur whereby an Internet search request inadvertently leads a user to an offensive website. This does not mean the University condones sexual harassment and offensive information. Users should exercise caution since even innocuous searches may lead to sites with offensive content;

2. Virginia State Policy DHRM 1.75 and Code §2.2-2827 specify that certain activities are prohibited. Among these include accessing, downloading, printing, or storing information with sexually explicit content;

3. Mindful of the Commonwealth guidance specified above, the University has implemented a widely used website scanning and blocking system. When users attempt to connect to websites that are on the list of blocked sites, access to the website is denied and a webpage is returned which informs the user that the site has been blocked. This webpage also provides information on how to contact a University representative if additional information or clarification is needed;

4. Users can request that access to blocked websites be permitted by submitting a request to

clientservices@nsu.edu. Requests are referred to the Information Systems Security Officer and reviewed by the Information Security Officer, or a designated representative, who then determines if the block should be removed or if additional review is required. Users are then advised of the follow-on action;

5. Special care should be taken when downloading files to protect computer systems from viruses, spyware, and other harmful software and computer code.

UNIVERSITY RECORDS

E-mail can be considered as public records in some situations. However, the University regards electronic mail as a vehicle for delivery of information and not as a mechanism for the retention and/or archiving of information. It is the responsibility of the senders and receivers of e-mail and attached documents to determine which information must be retained and for how long.

VIOLATIONS

Violations of this policy will be addressed in accordance with the Commonwealth of Virginia Policy Number 1.75 which is relevant to this policy. The appropriate level of disciplinary action will be determined on a case-by-case basis by the appropriate Vice President or designee, with sanctions up to or including termination or expulsion from the university depending on the severity of the offense.

INTERPRETATION

The Information Security Officer (or designee) is responsible for official interpretation of this policy. Questions regarding the application of this policy should be directed to Information Technology Services. The Information Security Officer reserves the right to revise or eliminate this policy.

PUBLICATION

This policy shall be widely published and distributed to the University community. To ensure timely publication and distribution thereof, the Responsible Office will make every effort to:

- Communicate the policy in writing, electronic or otherwise, to the University community within 14 days of approval;

- Submit the policy for inclusion in the online Policy Library within 14 days of approval;
- Post the policy on the appropriate Website; and

- Educate and train all stakeholders and appropriate audiences on the policy's content, as necessary. Failure to meet the publication requirements does not invalidate this policy.

REVIEW SCHEDULE

- Next Scheduled Review: 10/01/2021
- Approval by, date: President, 07/14/2014
- Revision History: 04/28/2015; 04/28/2016; 06/18/2016, 06/07/2017, 10/1/2018
- Supersedes (previous policy): OIT 60.201 and 48-01 (2014) Acceptable Use of Technological Resources

RELATED DOCUMENTS

Virginia Department of Human Resources Management Policy 1.75

http://www.dhrm.virginia.gov/docs/default-source/hrpolicy/pol175useofinternet.pdf?sfvrsn=2

Codes of Virginia §2.2-2827

https://law.lis.virginia.gov/vacode/title2.2/chapter28/section2.2-2827/