

3358: 14-13-01 Information technology.

- (A) This policy applies to all users of Northwest state community college (NSCC) computing resources, whether affiliated with NSCC or not, regardless of whether the user is on campus or off, regardless of the client used to access a resource, and regardless of the specific use of a resource. Additional policies may apply to specific computers, computer systems, or networks used by specific units of NSCC. All sections of this policy also apply to college publications on the Internet.
- (B) The college acquires, develops, and maintains computers, computer systems, and networks as a part of the educational, physical, and social learning infrastructure. The computing resources are intended for college-related purposes which include direct and indirect support of NSCC's instruction, research, and service missions; college administrative functions; student and campus life activities; and the free exchange of ideas among members of the college community and between the college community and the wider local, national, and world communities.
- (C) This policy establishes a college-wide information security program. This program develops and maintains standards and guidelines for the protection of information in compliance with all applicable laws and regulations.
- (D) The rights of academic freedom and freedom of expression apply to the use of college computing resources. However, as is true of any other college-provided resource and college-related activity, those rights do not supersede other binding requirements, responsibilities, and limitations of legal and ethical behavior. In particular, legitimate use of a computer, computer system, or network does not extend to whatever is technically possible. The limitations and constraints built into computer operating systems and networks are not the sole restrictions on what is permissible. Users must abide by all applicable restrictions, whether or not they are enforced mechanically or electronically, and whether or not they can be circumvented by technical means.
- (E) While NSCC encourages fully utilizing the internet in addition to traditional collections to access information and educational resources, not all sources on the internet contain information that is accurate, complete, current, legal, safe, or secure. The college does not endorse the viewpoints nor vouch for the accuracy of general information accessed through the

internet and cannot be held responsible for its content. Some resources and destinations accessed through the internet contain information that some people find offensive or objectionable. Internet users access sites at their own risk. Images viewed on screens in open labs and offices may be viewed inadvertently by a wide audience. NSCC is not responsible for the information accessed or displayed using college systems.

(F) NSCC recognizes the key role that information technology services plays in the learning process and individual development and realizes the key role technology plays in students' success. Therefore, information services access priority is given to academic and college-related work. Resources used for general interest that relate to educational material and learning is encouraged, but priority will be given to course-related usage.

(G) All users of college computing resources must:

- (1) Comply with all federal, state, and other applicable laws; all generally applicable college rules and policies; and all applicable contracts and licenses. Examples of such laws, rules, policies, contracts, and licenses include, but are not limited to, the laws of libel, privacy, copyright, trademark, obscenity, and child pornography; the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, which prohibit "hacking", "cracking", and similar activities; NSCC's code of student conduct; NSCC's sexual harassment policy; FERPA and HIPAA laws; and all applicable software licenses. Users who engage in electronic communications with persons in other states or countries or on other systems or networks should be aware that they may be subject to the laws of those states and countries and the rules and policies of those systems and networks. Users are responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses.
- (2) Use only those computing resources that they are authorized to use and only in the manner and to the extent authorized. Ability to access computing resources does not, by itself, imply authorization to do so. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding. Accounts and passwords may not, under any circumstances, be shared with, or used

- (3) by, persons other than those to whom they have been assigned by NSCC.
- (4) Respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected. The ability to access an account does not by itself imply authorization to do so. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding.
- (5) Respect the finite capacity of those resources and limit use so as not to consume an unreasonable amount of those resources or to interfere unreasonably with the activity of other users. NSCC may require users to limit or refrain from specific uses in accordance with this principle or for similar reasons.
- (6) Not use those resources for personal financial gain or commercial purposes which is strictly prohibited. Personal, non-commercial, use of college computing resources is permitted when it does not consume a significant amount of these resources, does not interfere with the performance of the user's job or other college responsibilities, and is otherwise in compliance with this policy. NSCC may limit personal use if needed.
- (7) Refrain from stating or implying that they speak on behalf of NSCC and from using college trademarks and logos without authorization. Affiliation with NSCC does not, by itself, imply authorization to speak on behalf of the college.
- (8) Policy violators may be denied access to college computing resources and may be subjected to other penalties and disciplinary action, both within and outside of the college. Violations will normally be handled through college disciplinary procedures applicable to the relevant user. For example, alleged violations by students normally will be investigated, and any penalties or other discipline normally will be imposed by the vice president of academics and student services. However, as a precaution the college may temporarily suspend or block access to an account prior to the initiation or completion of such procedures in order to protect the integrity, security, or functionality of

(9) college or other computing resources or to protect NSCC from liability. NSCC may also refer suspected violations of applicable law to appropriate law enforcement agencies.

(H) NSCC employs various measures to protect the security of its computing resources and of its users' accounts. Nevertheless, the college cannot guarantee such security. NSCC strongly encourages users to engage in safe and responsible computing practices by following all recommendations specified in the NSCC security program.

(I) NSCC strives to respect and protect the privacy of its information systems users. However, the college may access user data, private or not, for various reasons. While NSCC does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of NSCC'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 to provide service. NSCC may also specifically monitor the activity and accounts of individual users of college computing resources, including individual login sessions and communications, without notice, when:

- (1) It reasonably appears necessary to do so to protect the integrity, security, or functionality of college computing resources or to protect NSCC from liability.
- (2) There is reasonable cause to believe that the user is in violation of this policy. Reasonable cause includes, but is not limited to, appearance of unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns
- (3) It is otherwise required or permitted by law.
- (4) Monitoring other than that required by law or in response to a declared emergency must be authorized in writing and in advance by the president or her/his designee. Every effort will be made to keep those records private, unless disclosure is required by law. NSCC may

(5) disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate college personnel or law enforcement agencies and may use those results in appropriate college disciplinary proceedings. Communications made by means of college computing resources are also generally subject to Ohio's Public Records Statute, Ohio Public Record Act. O.R.C. 149.43 et seq., to the same extent as they would be if made on paper. At the termination of an individual investigative or monitoring process, both internally and externally of NSCC, the individual within NSCC who has been monitored will be notified of the monitoring activity, unless NSCC is legally restricted from doing so.

(J) Northwest state community college's world wide web pages are considered official college publications as well as campus-wide information sources. As with printed materials, web page content must be approved prior to being published on the college public web site.

(1) Northwest state community college (NSCC or college) strives to maintain a modern, comprehensive, and easy to navigate presence on the world wide web (web). This presence is intended to provide information and services in a timely and accurate manner to all its visitors. The web presence for NSCC will contain password-protected information as well as open-access information.

(2) Information presented on the web is a part of NSCC's official publications and shall remain in NSCC's control. Open-access pages shall conform to the established web presence standards. Password-protected pages designed for delivery of course content or specialized applications may deviate from the web presence standards as required by other established college standards. These procedures do not infringe on academic content decision-making criteria.

(3) The NSCC web presence will:

(a) Present a desirable image of NSCC specific to its mission and vision.

- (b) Provide faculty and students access to information resources available on and via the world wide web.
- (c) Disseminate official college information to all its audiences.
- (d) Before any content is published to any Northwest state community college web sites, the department requesting must select an individual as an information provider. That person or persons are responsible for the management of the information and coordination of the content and the request. Information providers are:
 - (i) Designated by the department head in all areas of Northwest state community college. More than one information provider may be designated by an area or department.
 - (ii) Trained on how to create and manage content using web content creation and management systems and the associated templates and standards.
 - (iii) Provided access to web content management systems by information technology with institutional advancement's approval.
 - (iv) Responsible for creating and maintaining their information and content.
 - (v) Accountable to ensure the content and information along with all web links they provide to their web sites are accurate, timely, and relevant to Northwest state community college and its stated mission, and are of highest value to students in meeting their Northwest state general education outcomes and/or specific course objectives.

- (K) Institutional advancement will maintain the user access approval process for maintenance and update of the online presence. Information providers must present a request to post the area/department's online content to institutional advancement using the designated forms and interfaces.
- (L) Institutional advancement will establish appropriate processes for approval and moving of the content submitted by the information providers to the appropriate sites. The decision whether content should be password protected may be made prior to submission by information providers or by institutional advancement.
- (M) Data protection standards established within NSCC's information security program must be adhered to when handling data as part of the content.
- (N) It is understood that NSCC may need to use delivered applications to provide online services to its users. When feasible, NSCC will customize these applications to adhere to web presence standards.
- (O) All online service applications regardless of their hosting environments must be reviewed for information security and contract management by the information technology department.
- (P) Web pages using the NSCC logo or college-owned content must be reviewed by the information technology department. Academic course content follows standards established by distance learning committee.
- (Q) Departments may need to request a specific uniform resource locator other than NSCC's url address: www.northweststate.edu. The rationale for this request must be provided to institutional advancement. If approved, the url address must be obtained through the information technology division.
- (R) No personal homepages on college open-access web sites will be permitted. Links to personal homepages are approved for academic use only.
- (S) Information providers and their respective departments are the owners of and responsible for their content. The information provider and the respective department are responsible to determine the propriety of all external links presented as part the department's online content.

(T) Institutional advancement bears responsibility for monitoring web content to ensure it is accurate, timely, and relevant to the college and its mission. Institutional advancement will assist any college area requesting support concerning the appropriateness of web content. Institutional advancement will also work to assure that the content of the web site and web links is of highest value to students in meeting NSCC's general education outcomes and/or specific course objectives.

(U) NSCC allows for social networking sites such as blogs, wikis, facebook, linkedin, youtube, flickr, etc. as part of its web presence subject to prior approval from institutional advancement. Institutional advancement will provide the requester(s) with site guidelines to ensure highest quality of social networking experience.

(V) Noncompliance with this or any other college policies or procedures may result in removal of files from the web servers.

(W) Administrative and academic units of NSCC are encouraged to develop. Units of the college must use the tools and frameworks sanctioned by NSCC to develop these web pages, and they must comply with NSCC's technical, business, and legal standards and obligations. Official college pages will be linked to appropriate, previously created categories within the Northwest state home page.

Effective: 03/16/2015

CERTIFIED ELECTRONICALLY

Certification

03/05/2015

Date

Promulgated Under: 111.15
Statutory Authority: 3358
Rule Amplifies: 3358