

Northern Oklahoma College

Student Information Technology Policy



NORTHERN
Oklahoma College

TONKAWA | ENID | STILLWATER

TABLE OF CONTENTS

| | |
|---|----|
| Overview | 3 |
| Purpose | 3 |
| Scope | 3 |
| Policy | 3 |
| 1 General Use and Ownership | 3 |
| 2 Acceptable Use | 4 |
| 2.1 Agreement Terms | 4 |
| 2.2 Additional Guidelines | 4 |
| 3 Network Use | 6 |
| 4 Technology Maintenance and Support | 7 |
| 4.1 Hardware | 7 |
| 4.2 Software | 7 |
| 4.3 Reliability and Network Maintenance | 8 |
| 5 Internet Access and Email | 8 |
| 6 Residence Hall Network Access | 9 |
| 6.1 Hardwired | 9 |
| 6.2 Wireless | 9 |
| 6.3 Gaming Support | 9 |
| 7 College Computer and Classroom Labs | 10 |
| 7.1 During Academic Breaks and Other Times | 10 |
| 7.2 Classroom Equipment | 10 |
| 8 Violations of this Policy | 10 |
| 8.1 Exceptions | 11 |

OVERVIEW

The Department of Information Technology is responsible for providing technology support to Northern Oklahoma College (NOC) and for the development and implementation of the college's information systems. Information technology is constantly changing in the way that people communicate, learn and share information. NOC is committed to using these innovations to provide new educational benefits to its students and to the NOC community.

PURPOSE

A computer network establishes a community, and as in any community, especially one as tightly linked as an electronic network, individual decisions can have a powerful and immediate impact on a large number of people. Accordingly, the community must develop rules and protocols to ensure that the rights and privileges of each member of the community are protected and that the college's investment in the technology is protected. Northern Oklahoma College stresses respect for all college technology and consideration for those who use the system. Use of Northern Oklahoma College technology is considered a privilege.

SCOPE

This policy applies to all students at Northern Oklahoma College when using the college's computing, network or technology services.

POLICY

1 GENERAL USE AND OWNERSHIP

- Student computer accounts are created at Northern Oklahoma College for all enrolled students; accounts are deleted when the student has not enrolled for class for two or more consecutive semesters.
- While Northern Oklahoma College desires to provide a reasonable level of privacy, users should be aware that the data created or stored on any computer workstation or server remains the property of NOC. Because of the need to protect the security of the NOC network and computer system, the college cannot guarantee the confidentiality of information stored on any network device belonging to the college.
- Computing resources shall be used in a manner consistent with the instructional and administrative objectives of the college. You are expected to use computing resources in a responsible and efficient manner.
- For security and network maintenance purposes, authorized individuals within Northern Oklahoma College may monitor equipment, systems and network traffic at any time to ensure compliance with this policy.

2 ACCEPTABLE USE

Transmission of any material in violation of any local, state or federal regulation is prohibited. This material includes, but is not limited to, copyrighted material, or threatening or obscene material. The use of Northern Oklahoma College technology for political lobbying is also prohibited. Any use of college computers and servers to transmit material that may be perceived as sexual in nature may be considered a violation of the college's sexual harassment policy as well as the technology policy. NOC reserves the right to direct that the transmission of any sexually inappropriate material be ceased and to remove the material itself if necessary. NOC has the right to remove any material that is contrary to the college's mission or is otherwise deemed inappropriate. Students bear the responsibility of knowing what activities are prohibited by state and federal law, federal copyright and trademark laws, stalking laws and software piracy laws.

2.1 AGREEMENT TERMS

As a user of the Northern Oklahoma College's local and shared computer systems, students must abide by the following acceptable use agreement terms. These terms govern the access to and use of the information technology applications, services and resources of Northern Oklahoma College and the information they generate.

The college has granted access as a necessary privilege in order to perform authorized functions. Students are not to knowingly permit use of entrusted access control mechanisms for any purposes other than those required to perform authorized functions related to the status as a student. These include log-on identification, password, workstation identification, user identification, or digital certificates.

Students must use only those computer resources that they have the authority to use. Students must not provide false or misleading information to gain access to computing resources. Northern Oklahoma College may regard these actions as criminal acts and may treat them accordingly. Students must not use NOC technology resources to gain unauthorized access to computing resources of other institutions, organizations, individuals, etc.

If a student observes any incidents of non-compliance with the terms of this agreement, they are responsible for reporting them to the Department of Information Technology.

Each student is responsible to read and abide by this agreement, even if they do not agree with it. If a student has any questions about the Northern Oklahoma College Information Technology Acceptable Use Agreement, they may contact the Department of Information Technology.

2.2 COPYRIGHT & ADDITIONAL GUIDELINES

Computer software, databases, and electronic documents are protected by copyright law. A copyright is a work of authorship in a tangible medium. Copyright owners have the sole right to reproduce their work, prepare derivatives or adaptations of it, distribute it by sale, rent, license lease, or lending and/or to perform or display it. A student must either have an express or implied license to use copyrighted material or data, or be able to prove fair use. Students are responsible for understanding how copyright law applies to their electronic transactions. They may not violate the copyright protection of any information, software, or data with which they come into contact through the college computing resources. Downloading or distributing copyrighted materials such as documents, movies, music, etc. without the permission of the rightful owner may be considered copyright infringement, which is illegal under federal and state copyright law. Use of the college's network resources to commit acts of copyright infringement may be subject to prosecution and disciplinary action.

Unauthorized distribution of copyrighted material, including peer-to-peer file sharing, may result in internal disciplinary adjudication, civil or criminal liabilities. Peer-to-peer (P2P) file sharing allows users to make files available to others for download and use. Copyright infringement may occur through the practice of copying and distributing protected work without the permission of the owner. This material includes any software belonging to the user or software located on the Northern Oklahoma College system. Any instances of peer-to-peer file sharing found on Northern Oklahoma College's network will be terminated immediately. When the student has removed the offending P2P software the student's network access can be restored. Any internal action taken by NOC does not shield a student from potential liability claims from third parties.

The penalties for infringing copyright law can be found under the U.S. Copyright Act, 17 U.S.C. (<http://www.copyright.gov/title17/>) and in the U.S. Copyright Office's summary of the Digital Millennium Copyright Act (<http://www.copyright.gov/legislation/dmca.pdf>).

- Students should not attempt to gain access to information owned by the college or by its authorized users without the permission of the owners of that information.
- Accessing, downloading, printing, or storing information with sexually explicit content is prohibited;
- Downloading or transmitting fraudulent, threatening, obscene, intimidating, defamatory, harassing, discriminatory, or otherwise unlawful messages or images is prohibited;
- To respect the financial structure of a telephone, computing, or networking system; for example, you shall not develop or use any unauthorized mechanisms to alter or avoid charges levied by the college or any of its providers.
- Sending e-mail using another's identity, an assumed name, or anonymously is prohibited;
- Attempting to intercept or read messages not intended for the student is prohibited;
- Intentionally developing or experimenting with malicious programs (viruses, worms, spy-ware, keystroke loggers, phishing software, Trojan horses, etc.) on any college-owned computer is prohibited;
- Students should not attempt to exploit, test, or probe for suspected security holes on Northern Oklahoma College computers or networks, but instead should report them to the Department of Information Technology. Likewise, students should not disseminate to others any information that serves to circumvent or degrade system or network security or integrity.
- Knowingly propagating malicious programs is prohibited;
- Changing administrator rights on any college-owned computer, or the equivalent on non-Microsoft Windows based systems is prohibited;
- Using college computing resources to support any commercial venture or for personal financial gain is prohibited.
- Physical theft, rearrangement, or damage to any college computer or network equipment, facilities, or property is strictly prohibited, and will be reported to the police. This includes all public computer labs, network hubs, wiring, and links.

Northern Oklahoma College reserves the right (with or without cause) to monitor, access and disclose all data created, sent, received, processed, or stored on NOC systems to ensure compliance with NOC policies and federal, state, or local regulations. College officials will have the right to review and/or confiscate (as needed) any personal equipment connected to an NOC-owned device or network.

The Department of Information Technology must ensure that academic work takes precedence at all times over other computing activities in its facilities. In situations of high user demand that may strain available computer resources, the Department of Information Technology reserves the right to restrict (e.g., to specific times of day) or prohibit computer entertainment activities such as game playing. Similarly, loud or disruptive behavior that may hinder academic work in the computer labs is not permitted.

Violation of any of these guidelines will be sufficient grounds for the suspension and/or termination of service and possible referral to other sanctioning or enforcement units. The examples provided above are not intended to be an exhaustive list of actions that might violate this policy.

3 NETWORK USE

Northern Oklahoma College utilizes this technology policy to inform students that unsecured wireless access points established using the NOC-provided hardwired network are prohibited. If unsecured wireless access points are detected, the originating IP address will be suspended without notification. Connectivity may be re-established at the discretion of the Department of Information Technology. Any device attached to the network must be configured as a DHCP client. The use of static addressing or configuring services that provide addresses in place of those assigned by NOC is prohibited. Students may not disconnect NOC hardware from the NOC network for any reason. Authorized users may not run or otherwise configure software or hardware that allows access to unauthorized users. This includes, but is not limited to, the creation of unsecured wireless networks, replication of services through third-party devices, such as routers, NAT devices and proxy servers, and the establishment of VPN services. Any placement of a device designed to extend the network must be configured to allow only the authorized user and must not be open to the public or to anyone other than the authorized user. Users are solely responsible for their connection and all traffic generated and received by that connection. Violations of this technology policy may result in the loss of user access privileges.

Additional Information & Guidelines

- Contact the Department of Information Technology with questions or concerns about whether a specific use of the network is authorized.
- Students with personal computers on the NOC network are expected to take reasonable precautions to ensure the security of their systems. Individuals may be held responsible for misuse by others that occurs on their systems.
- Northern Oklahoma College reserves the right to scan the NOC network and systems connected to it to assist in identifying and protecting against exploitable security vulnerabilities (e.g., viruses) and to preserve network integrity and availability of resources (e.g., sufficient bandwidth). Computers may be disconnected from the network until security issues have been resolved. Students may not scan NOC network or computers that they do not own or officially administer.
- Attempts to monitor, analyze, or tamper with network data packets that are not explicitly addressed to your computer are prohibited.
- Using a network address other than the one assigned by NOC is prohibited.
- Students are not permitted to register external domain names (i.e., any domain outside of noc.edu) that reference systems on the NOC network without authorization.
- Students may not advertise routing information on the NOC network or act as gateways to external or private networks.
- Providing services or running applications that consume excessive bandwidth or impede others' use of the NOC network is prohibited without authorization.

- The creation and propagation of viruses or malware, the creation of self-replicating code, port scanning, and other unsafe activities that disrupt services, damage files, and damage or destroy equipment, software or data are strictly prohibited.
- Students of the college's network are prohibited from the installation of devices or software designed to intercept, capture, and cache or otherwise acquire data transmissions through the NOC's network.

4 TECHNOLOGY MAINTENANCE AND SUPPORT

Malfunctions or suspected malfunctions should be reported to the Department of Information and Technology Help Desk for immediate attention. All repairs and modifications to Northern Oklahoma College technology are to be conducted by Northern Oklahoma College IT staff, or by Northern Oklahoma College IT-approved service providers.

4.1 HARDWARE

Northern Oklahoma College hardware (i.e., CPU, monitor, access point, keyboard, mouse, printer, scanner and other peripherals) represents a large investment of funds and provides the student body with an extensive array of tools to facilitate success at NOC. An equipment malfunction is costly to repair and makes the item unavailable to other users. For this reason, students should treat all equipment with the same respect and care allotted to personally owned equipment. Respecting the physical integrity of the hardware means students shall not tamper with, remove or add any piece or part of a piece of hardware or its accessories (inks, paper, cabling, etc.) from its proper location.

4.2 SOFTWARE

All installation of software is the responsibility of the Department of Information Technology. No one may attempt to install executable programs or applications without authorization from IT. No one should attempt to introduce system-corrupting software (such as viruses) into any computer system or otherwise intentionally interfere with the operation of any Northern Oklahoma College computer system. Northern Oklahoma College licenses the use of computer software from a variety of outside companies. Software purchased by NOC may only be used for educational purposes. The software may not be used for any commercial purpose, including any use where the student receives compensation or in-kind donations as a result of using NOC software. Students shall use the software only in accordance with the official license agreements. Students shall not download or upload unauthorized software on any NOC computer. Any student learning of any misuse of software should notify the Department of Information Technology.

4.3 RELIABILITY AND NETWORK MAINTENANCE

Northern Oklahoma College makes no warranties of any kind, whether expressed or implied, for the technology it provides. NOC is not responsible for any monetary or emotional damage suffered by a student as a result of system failure. This includes loss of data, software or hardware system delays or failures, file transfer failures, or service interruptions. Use of any information obtained via the system or the Internet is at the user's own risk. The network and available systems require regular maintenance to maintain reliability and current capacity. It is occasionally necessary for the Department of Information Technology to interrupt network availability in order to perform upgrades and maintenance. If upgrades or maintenance are required, email notifications will be sent to the students' Northern Oklahoma College email address in advance, outlining the projected unavailability of the network, whenever possible.

5 INTERNET ACCESS AND EMAIL

Access to Internet and email are provided as a service to students of the college. These services are to be used for college purposes only. All other uses are prohibited. Northern Oklahoma College-issued email accounts should not be used or referenced in commercial activity. An NOC email account is automatically issued within 24 hours to students upon enrollment. Timely communications from various departments are emailed to students through NOC email; *students are responsible for checking their Northern Oklahoma College email daily*. All student communications internal to NOC and its employees shall be sent directly to the student's official NOC email account rather than any third-party email accounts (i.e., Gmail, Yahoo, etc.).

The following email and communication activities are strictly prohibited:

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Use of unsolicited email originating from within Northern Oklahoma College's networks or other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by NOC or connected via NOC's network.

Currently, the three greatest threats to information security are phishing, portable device loss and third-party data storage. The greatest of these is phishing. Phishing is the act of sending emails designed to trick individuals into providing credentials or clicking a malware-laced link or attachment. These emails often appear to be from a trusted individual or known organization. NOC students should be vigilant regarding suspicious emails and not open any attachments or links within unexpected emails. Such suspicious emails that are sent to Northern Oklahoma College-hosted student email accounts should be forwarded to the Department of Information Technology Help Desk for verification of legitimacy. If it is determined that a student email account is compromised due to phishing, the Department of Information Technology will temporarily disable the account for the protection of the student and any information stored within the account in question.

6 RESIDENCE HALL NETWORK ACCESS

Northern Oklahoma College students living in the college's residence halls are provided with a network connection.

6.1 HARDWIRED

In order for students to obtain access to the network through a provided network access jack, they must first have a network-ready computer and then take the following steps:

- Obtain and utilize an Ethernet network cable.
- Connect the computer/device to one of the two network jacks located in the residence hall room using the cable. Single residence hall rooms will only have one network jack.
- Start the computer.

NOTE: For security purposes each jack is configured to have only one device utilized on that jack. Students cannot plug-in one device and later plug in a different device.

6.2 WIRELESS

For wireless access, students must have a wireless network-ready computer and perform the following steps:

- Power on the computer and view available networks.
- Connect to "NOC" or "NOC Wireless."
- Log in to the Northern Access wireless site that appears in the browser using the student's Northern Access username and password.

Creating a secondary physical network using devices including bridges, routers, or wireless access points connected to the NOC network will not be supported by the NOC's IT Department.

If a student has a problem connecting to the network, he or she should call the Department of Information Technology Help Desk. It is the responsibility of the student on the college's network to protect personal equipment from intrusion attempts, electrical damage or software-driven attacks. Northern Oklahoma College has no obligation to provide, maintain, service, replace or otherwise be responsible for physical or software-driven damage to personal equipment in use on the Northern Oklahoma College network or any other network.

6.3 GAMING SUPPORT

The Department of Information Technology will not support guaranteed reliability of access and speed, as well as configuration assistance to the network, in the residence halls for the purposes of gaming.

7 COLLEGE COMPUTER AND CLASSROOM LABS

7.1 DURING ACADEMIC BREAKS AND OTHER TIMES

All Northern Oklahoma College computer labs, except computers located in the NOC Library, are closed between academic semesters while classes are not in session. During these breaks, students are not allowed to use these labs. Labs also may be inaccessible at other times due to required maintenance. As schedules may change, students should consult noc.edu/libraries for current library hours. In order to use a Northern Oklahoma College computer lab, currently enrolled students must log in with their Northern Access username and password.

7.2 CLASSROOM EQUIPMENT

The Information Technology staff maintains technology located within classrooms and laboratories. Students are encouraged to report situations involving technology that is inoperable or in need of repair to the Information Technology Help Desk ((580)628-6291). The IT staff relies on this communication to provide fast and efficient service and to maintain the highest standard for classroom technology.

Northern Oklahoma College has platform manager software installed in all of its student computer labs. This software allows the IT Department to manage and secure these labs. Students should not save personal files to the computers in these labs. Northern Oklahoma College is not responsible for lost or damaged personal files created or stored on these lab computers.

Students are prohibited from using or troubleshooting the technology equipment used for instruction in NOC's classrooms. Instructors and classroom facilitators are to contact the IT Help Desk for assistance.

8 VIOLATIONS OF THIS POLICY

Any student found to have violated this policy may be subject to disciplinary action through the Office of Student Affairs, up to and including expulsion. Northern Oklahoma College students are required to report any instances where the violation of policies is occurring or has the potential to occur. The Department of Information Technology will investigate the alleged violation. In order to prevent further possible unauthorized activity, Northern Oklahoma College may suspend the authorization of computing services access to the individual or account in question.

Northern Oklahoma College reserves the right to terminate access at any time to any student whose use of its resources violates the law or threatens system or network security, performance, or integrity. This includes the ability to terminate running processes or active connections.

8.1 EXCEPTIONS

In rare cases, exceptions to this policy may be granted, but will not be considered without written approval from the Director of Information Technology. Additional approvals may also be necessary.