INTRODUCTION

The information, computing, and instructional technology resources provided by NSU are intended to assist members of the NSU community faculty, students, and staff in the fulfillment of their educational responsibilities. These resources and their effective use, contingent upon first amendment and academic freedom principles that demand the free flow of information and a free and open atmosphere, are vital to the mission of NSU. Such use is encouraged; however, since these resources are state property, their use is a privilege. For all to benefit, proper and fair use is necessary.

PURPOSE

The purpose of this policy is to outline the rights and responsibilities of both NSU and the users of these resources.

TARGET AUDIENCE

The NSU IT Acceptable Use Policy applies to NSU faculty, staff and students as well as external constituents that utilize NSU technology resources.

POLICY

- NSU Responsibilities
  - NSU has the responsibility to maintain a reasonably stable and secure network environment. Scheduled downtime will be limited and well announced.
  - NSU has the responsibility to backup files and data stored on the campus network on a regular basis. Users should be aware, however, that no system configuration, backup process or security setup is 100% effective.
• Network and computing equipment (hardware and software) provided by NSU will be legally obtained, up-to-date and sufficient for the needs of users.

• NSU intends that all uses of information resources and technology support the operations and mission of the university. While doing so, the statutory rights of the individuals will be safeguarded. Ownership resides with the University and data in the system may be subject to discovery during litigation and disclosed in court proceedings.

• NSU cannot guarantee the security, privacy, and confidentiality of electronic data, including e-mail. Users should not assume confidentiality of their data and e-mail. Users are advised not to send confidential University communications (as determined by law, policy, etc.) via e-mail. Examples of why data and e-mail confidentiality cannot be guaranteed include:
  - E-mail and data may be subject to disclosure under law;
  - Back-up copies may be retained for periods of time and in locations unknown to senders and recipients even if the user has deleted it from their account or PC;
  - In the course of routine systems maintenance and troubleshooting, network or systems staff may inadvertently see the content of e-mail messages or data files;
  - Password protections are advised but cannot be guaranteed; and
  - E-mail messages and electronic files can be forwarded without permission to individuals or groups.

• **User Responsibilities**
  • Users have a responsibility to backup files and data stored on their personal office machines on a regular basis.
  • Users have a responsibility to ensure that their computing devices are physically and electronically secure.
  • Users have a responsibility to treat other users and the staff with consideration and respect. Abuse or harassment of others will not be tolerated. Users should be sensitive to the diverse and public nature of facilities.
  • Since users have a right to resources sufficient to their needs, they have a responsibility not to use excessive resources. This would include chain letters, spam, mass mailings, and excessive printing, game playing, P2P, or otherwise unnecessary network traffic. In addition, users must only keep NSU business/academic related documents on the home directory (F: drive) and other file server storage locations.
  • Users have a responsibility to manage their data appropriately by occasionally reviewing contents and removing outdated, duplicated or otherwise unnecessary files to ensure that this resource is reliable and available.
  • Users must obey the law. Under state and federal laws, the following activities are illegal: distribution or retrieval of child pornography, distribution of pornography to minors, obscenity, scams and pyramid schemes, copyright infringement, and unauthorized duplication of software. Users have the responsibility not to use illegally obtained or pirated software. Copyright and intellectual property laws must be obeyed (for additional information on copyright and intellectual property law, see the library home page (refer to actual document). Proof of ownership must be provided to staff prior to installing or helping with software.
  • Users have a responsibility not to abuse or mistreat equipment or data or to use networks and accounts or access data for which they do not have authorization. This includes any form of computer hacking.
- Users are to take precautions to prevent the unauthorized use of all account passwords. Passwords are not to be shared with others and their confidentiality is to be strictly maintained. Users will be held accountable for all actions performed with their passwords, including those performed by other individuals as a result of user negligence in protecting codes.

- Users must exercise caution to ensure their private and privileged information is not exposed to inadvertent disclosure.

- Northern State University treats policy violations of computing facilities, equipment, software, information resources, networks or privileges seriously. Disciplinary action resulting from such abuse may include the loss of computing privileges and other sanctions including non-renewal, discharge, and dismissal. Alleged violations of the policy shall be processed according to the judicial processes outlined in the SDBOR/COHE Higher Education Contract, the Faculty Handbook, and the Student Handbook.

- Where the facts that would trigger disciplinary action under this policy may also constitute a criminal infraction under state and federal law it may be reported to responsible authorities, whether or not disciplinary action is initiated.