Policy title	Category
Responsible Use of University Computers and Information Systems	Administration Information Technology
Owner	**Approved by**
ITS	Ad Council

Purpose of this policy

It is the purpose of this Policy to set forth the Nebraska Wesleyan University (“University”) policy and provide guidance relating to responsible use of the University’s devices and electronic Information Systems. This policy serves as the University’s definitive statement on the use of electronic devices, software, and information systems within the academic and employment setting of the University.

Policy statement

The University strives to maintain access to local, national, and international sources of information for its faculty, staff, students, administrators, board of governors, and others with approved access (“users”), and to provide an atmosphere that encourages sharing of knowledge, the creative process, and collaborative efforts within the University’s educational mission. Access to and use of electronic information systems and University devices at the University is not a right but is a benefit of employment which may be removed at the sole discretion of the University in the event of misuse or violation of this policy. All users must act honestly and responsibly. Every user is responsible for the integrity of these information resources. All users must respect the rights of other computer users, respect the integrity of the physical facilities and controls, and comply with all pertinent license and contractual agreements related to the University’s information systems. All users shall act in accordance with these responsibilities, and the relevant local, state, and federal laws and regulations.

The University is a provider of a means to access the vast and growing amount of information available through electronic information resources. The University is not a regulator of the content of that information and takes no responsibility for the content of information, except for that information the University itself and those acting on its behalf create. Any person accessing information through the University’s information systems must determine for themselves and their charges whether any source is appropriate for viewing.

Accessing any account and/or using the University’s information system shall constitute an agreement on behalf of the user or other individual accessing such information systems to abide and be bound by the provisions of this policy. The University may restrict or prohibit the use of its information systems in response to complaints presenting evidence of violations of University policies or state or federal laws. When it has been determined that there has been a violation, the University may restrict or prohibit access by an offending party to its information systems through University-owned or other computers, remove or limit access to material posted on University-owned computers or networks, and, if warranted, institute other disciplinary actions.

A fundamental premise of this policy is that anyone sharing computing resources with other individuals should behave as a reasonable, mature and ethical person. The user must recognize that computer systems and networks do not exist in a special environment; on the contrary, use of computers is a form of communication, and every component of a computing environment and every piece of information it contains belong to the university, the university community as a whole, or some individual or group within that community.

For each of the areas addressed in this policy, it is possible an exception may need to be considered in the event of emergencies or unique business acumen. In these cases, see section 19 for the exception approval process.

Definitions
For purposes of this Policy the following definitions shall apply:

a. Electronic communications shall mean and include the use of information systems in the transmitting, receiving, storing, or posting of information or material by way of email, message boards, forums, chat, websites, institutional social media accounts, or other such electronic tools over the Internet or other networks.

b. Information systems shall mean and include endpoints, networks, systems, services, and other similar devices that are administered, owned, or operated by the University or for which the University is responsible.
* Endpoints shall refer to desktops, laptops, tablets, mobile devices, printers, or any other device, excluding servers, capable of connecting to the University network or accessing University data.
** Networks shall mean and include wired and wireless video, voice, and data infrastructure, including security devices.
*** Systems shall mean and include software, server, storage, licensed platforms, and cloud-based services.

c. University devices shall mean and include any device purchased with university funds (including but not limited to state, foundation, grant, contract, etc.) capable of connecting to University networks directly or through a gateway. Examples include, but are not limited to, desktops, laptops, tablets, printers, IoT devices, servers, appliances, and sensors.

d. Bring Your Own Device (BYOD) shall pertain to personally owned endpoints used to connect to and access University information systems.

e. Removable Media shall mean devices or media that is readable and/or writable by the end user and are able to be moved from computer to computer without modification to the computer. Examples can be found in the ITS-12: Removable Media/Media Protection Standard Process.

f. Records and Data are defined in ITS-02: Risk Classification Standard and includes institutional and research data.

g. Obscene with respect to obscene material shall mean: (1) that an average person applying contemporary community standards would find the material taken as a whole predominantly appeals to the prurient interest or a shameful or morbid interest in nudity, sex, or excretion, (2) the material depicts or describes in a patently offensive way sexual conduct specifically set out in Neb. Rev. Stat. §§ 28-807 to 28-809, as amended, and (3) the material taken as a whole lacks serious literary, artistic, political, or scientific value.

Permitted Uses

a. University Business Use and Limited Personal Use. University information systems are to be used predominantly for University-related business. However, personal use is permitted so long as it conforms with this policy and does not interfere with University operations or an employed user's performance of duties as a University employee. Personal use of any University information system to access, download, print, store, forward, transmit, or distribute obscene material is prohibited. Under all circumstances, personal use by employees must comply with subsection b. of this section and shall not conflict with an employee's performance of duties and responsibilities for the University. Personal use may be denied when such use requires an inordinate amount of information systems resources (e.g., storage capacity or network bandwidth).

b. Priority Approval Required for Personal Use for Outside Consulting, Business, or Employment. Personal use of University information systems resources or equipment by any user for personal financial gain or in connection with outside (non-University) consulting, business, or employment is prohibited, except as authorized for employees by the University's Additional Employment Policy. Employee personal use in conjunction with outside professional consulting, business, or employment activities is permitted only when such use has been expressly authorized and approved by the University president, provost or vice president, the employee's supervisor, and documented with the Office of Human Resources, as appropriate.

Access

Unauthorized access to information systems is prohibited. No one shall use the identity of another (individual account); nor shall anyone provide their individual account authenticators/passwords to another. As individuals' relationships with the University change or terminate, their authorization to systems, services, and data shall be adjusted in accordance with University Administration or other University policies.

In situations where a shared account is requested, the requestor will be required to submit an exception process in accordance with ITS-01: Policy Exception Standard Process.

Misuse of Computers and Network Systems

Misuse of any University information system is prohibited. Misuse includes, but is not limited to, the following:

a. Attempting to modify or remove endpoint equipment, software, or peripherals without proper authorization.
b. Tampering with, willful destruction of or theft of any computer equipment, whether it belongs to the university or to an individual. Tampering includes any deliberate effort to degrade or halt a system, to tie up a system or to compromise the system/network performance. Willful destruction includes any deliberate disabling or damaging of computer systems, peripheral equipment such as

scanners or printers, or other facilities or equipment including the network, and any deliberate destruction or impairment of software or other users' files or data.

c. The unauthorized removal of university or another's computing equipment, which constitutes theft.

d. Accessing information systems without proper authorization, including information systems associated with the University, regardless of whether the resource accessed is owned by the University or the abuse takes place from a University site. (e.g. breaking into a system or using programs to obtain "root" access)

e. Taking actions, without authorization, which interfere with the access of others to information systems (e.g. "ping flooding" another system, sending "mail bombs," or modifying a login file in order to cause a user to not be able to log in).

f. Using a computer system without proper authorization granted through the university or department management structure. Some activities such as "port scanning" are not expressly prohibited. However, if the target of such scanning requests that an individual or system stop performing such actions, the person or system performing the scans must stop scanning the target machine unless the scans are being carried out by a system administrator who has the authority and responsibility over the machine(s) being scanned or for the network being used.

g. Using another person's computer account, files, or data without appropriate permission, as described in the previous bullet (e.g. using an account found "logged in" on a cluster machine).

h. Circumventing authentication and authorization controls.

i. Attempting to "crack" or guess other users' passwords. System administrators or those specifically designated by the administrator or owner of a system may attempt to crack passwords in order to test and enhance the security of the system. In cases where an individual or department "owns" machines which use password files controlled by another organization (e.g. Lab machines or their like), the owner may not attempt to crack passwords without explicit permission by the owners of the password database.

j. Obtaining passwords by other means, such as password capturing and key logging programs.

k. Using information systems for any illegal or unauthorized purpose.

l. Circumventing security measures required for information systems to meet security standards.

m. Storing, processing, analyzing, transmitting, or receiving University records and data on information systems that do not meet minimum security standards for the data classification as defined in the ITS-02: Risk Classification Standard.

n. Personal use of information systems or electronic communications for personal financial gain or non-University consulting, business, or employment, except as expressly authorized pursuant to Additional Employment Policy.

o. Sending any fraudulent electronic communication.

p. Violating any software license or copyright, including copying, or redistributing copyrighted software, without the written authorization of the software owner.

q. Using electronic communications that violates the property rights of authors and copyright owners.

r. Using electronic communications to harass or threaten users in such a way as to create an atmosphere which unreasonably interferes with the academic or employment experience. Similarly, electronic communications shall not be used to harass or threaten other information recipients, in addition to university users.

s. Sending commercial solicitations via email (i.e. spamming) to individuals, or to newsgroups or mailing lists where such advertising is not part of the purpose of the group or list. (It is permissible to send a commercial solicitation to a "for sale" newsgroup, provided that the advertisement conforms to other policies and guidelines at Nebraska Wesleyan.)

t. Any "mass mailing" which is solicitous in nature, unless the mailing is in the conduct of university business.

u. Reselling of services based on the university network, such as web hosting, mailing services or the selling of shell accounts.

v. Using electronic communications to disclose proprietary information without the explicit permission of the owner except as required by law, example law enforcement subpoena or search warrant.

w. Running a proxy server which results in inappropriate or unauthorized access to university materials to non-university members.

x. Advertising commercial businesses or ventures on Web pages hosted by Nebraska Wesleyan, unless prior authorization has been granted.

y. Accessing other users' information systems, information, or files without their express permission except as permitted in Section 7 below.

z. Deleting or tampering with another user's files or with information stored by another user on any information-bearing medium (disk, tape, memory, etc.). Even if the user's files are unprotected, with the exception of files intended for public reading, such as Web pages, it is improper for another user to read them unless the owner has given permission (e.g. in an announcement in class or on a computer bulletin board).

aa. Academic dishonesty; see related university policy.

bb. Forging, fraudulently altering or falsifying, or otherwise misusing University or non-University records (including computerized records, permits, identification cards, or other documents or property).

cc. Using information systems to hoard, damage, or otherwise interfere with academic resources available electronically.

dd. Using information systems to steal another individual's works, or otherwise misrepresent one's own work.

ee. Using information systems to fabricate research data.

ff. Launching a computer virus, malware, phishing attack, or other rogue or malicious program.

gg. Downloading or posting illegal, proprietary, or damaging material to a University endpoint.

hh. Transporting illegal or damaging material or proprietary material without authorization across a university network.

ii. Personal use of any University information systems to access, download, print, store, forward, transmit, or distribute obscene material.

jj. Violating any state or federal law or regulation in connection with use of any information systems.

This list should not be considered to be complete or exhaustive. It should, however, serve as a set of examples of inappropriate behaviors. If you are in doubt about the appropriateness of something that you want to do, contact support [at] nebrwesleyan.edu (support[at]nebrwesleyan[dot]edu) and ask first.

Privacy

a. User Privacy Not Guaranteed. The University is committed to respecting the privacy of individuals and will safeguard information about individuals subject to limitations imposed by federal and state law and other provisions. Members of the University community should respect the privacy of other community members, regardless of whether their accounts are securely protected; respect the privacy of all individuals for whom the University maintains records; and refrain from invading the privacy of individuals or entities that are creators or authors of information resources. The University employs numerous measures to protect the security of its IT resources and user accounts. Users should be aware, however, that no information system is completely secure. Persons both within and outside the University may find ways to access files.

Accordingly, the University cannot and does not guarantee user privacy, and users should be continuously aware of this fact. The University retains the right to review files, emails, and data for compliance with policy and its procedures. University IT system administrators will only act on this right for business purposes involving employment actions, legal subpoenas and warrants, or reasonable suspicion of harmful activities to the University. Actions taken due to reasonable suspicion of harmful activities must be approved by a member of University Administrative Council and CIO. Use of University information systems constitutes acknowledgement that users have no expectation of privacy, and consent to university review.

b. Repair and Maintenance of Equipment. Users should be aware that on occasion duly authorized University information technology personnel have authority to access individual user files or data in the process of performing repair or maintenance of computer equipment the University deems is reasonably necessary, including the testing of systems in order to ensure adequate storage capacity, performance, and security for University needs. Information technology personnel performing repair or maintenance of information systems are prohibited by law from exceeding their authority of access for repair and maintenance purposes or from making any use of individual user files or data for any purpose other than repair or maintenance services performed by them.

c. Response to a Public Records Request, Administrative or Judicial Order, Law Enforcement Investigations and/or Subpoenas, or Requests for Discovery in the Course of Litigation. Users should be aware that the Nebraska public records statutes are very broad in their application. Certain records, such as unpublished research in progress, proprietary or trade secret information, and personal information in personnel and student records are protected from disclosure. This does not apply to all electronic records or communication, including email. Users should remember this when creating any electronic information, especially email. Also, users should be aware that the University will comply with any lawful administrative or judicial order requiring the production of electronic data and records stored in the University's Information Systems and will provide information in electronic files or data stored in the University's Information Systems in response to legitimate requests for discovery of evidence in litigation.

d. Response to Misuse of Information Systems or Violations of University Policy. The University has a responsibility to monitor, audit, and ensure the proper use of those resources. Although the University supports a climate of trust and respect, it must monitor systems for misuse. Therefore, users of the University electronic information resources should not have an expectation of privacy in data, email, or other information transmitted or stored on University electronic information resources. Moreover, the University does not guarantee the confidentiality or security of data, email, or other information transmitted or stored on University electronic information resources. When University officials believe a user may be using electronic information resources in a way that may violate University policies or federal, state, or local law, or the user is engaged in activities inconsistent with the user's University responsibilities, or for other good cause, and upon review by and with the concurrence of University Administration, then the Chief Information Officer (CIO) serving the Nebraska Wesleyan University or the CIO's designee may monitor the activities and inspect and record the files of such users'(s) University devices, information systems, and applications. If the CIO reasonably believes that an act of misuse as defined in Section 6 above is present or imminent such that the potential for damage to the system or the information stored within it, is genuine and serious (e.g., hacking, spamming, or theft), then the CIO or the CIO's designee may take such action as is necessary to protect the information system and the information stored in it, including the denial of access to any University or non-University user, without prior review from University Administration; provided however, that the CIO shall notify associated Administrative Council member(s) as soon as possible to confirm that any protective actions taken were appropriate and within the parameters of this policy.

e. Access to Information Concerning Business Operations. Employees regularly carry out the business functions of the University using the University's information systems. Business records, inquires, and correspondence are often stored such that individuals may control the access to information stored within the University's information system. Should any employee become unavailable, be incapacitated due to illness or other reasons, or refuse to provide the information necessary to carry out the employee's job responsibilities in a reasonably timely manner, then following consultation with and approval by the University Administration, may authorize access to the employee's data and records in order to carry out University business operations on behalf of the unavailable or uncooperative employee. Any access to intellectual property of the employee must adhere to the University's Intellectual Property Policy in terms of duration and use.

Email

a. University Business. University faculty and staff must use University email accounts for University Business communication as defined in Section 10 of this policy.

b. Email Forwarding. Email sent to a University-provided email service or University-provided address shall not be forwarded through any automated means or service to a non-University-provided email address.

c. A University user may manually forward selected email to a non-University-provided email address when such forwarding:

*Will not result in an inappropriate disclosure of Medium-risk or High-risk data, as defined in ITS-02: Risk Classification Standard.
**Does not also automatically delete the email from the University-provided email system; and
****Complies with all other requirements of this policy.

d. Email Retention. Email messages should be deleted once the information contained in them is no longer useful or required to be retained by records retention schedules. Email messages stored in one or more backup files for business continuity (e.g., inadvertent or mistaken deletions or system failures) shall be retained for a period of time not to exceed ninety days.

Websites, Apps, and Digital Content

Nebraska Wesleyan University has established brand identity standards for websites and pages published from the official internet domains of each entity (nebrwesleyan.edu). Similarly, mobile and web apps developed for and representing the institution must also comply with these standards. These are considered to be “official” publications of the University. All official websites, apps, and other digital properties owned by the University shall prominently display the University’s logo to identify it as an official University digital property. No other digital properties shall be allowed to use University logos without the express written permission of the University. Publishers of any website, app, or digital content developed on behalf of the University shall comply with University policies and all federal, state, and local laws and regulations, including copyright laws, accessibility laws, obscenity laws, laws relating to libel, slander, and defamation, and laws relating to piracy of software. Further, publishers must comply with privacy and security policies, and any other relevant policies as defined by the University or its campuses. Publishers are responsible for the accuracy of content. Content should be reviewed on a timely basis to assure continued accuracy. All websites and apps must include a means by which users may provide feedback to the content publishers. The University and its campuses may maintain accounts on external services hosting social, informational, and other content. In general, these accounts are the property of the University, administrative unit, or the department or unit that maintains them. All content provided through these accounts shall be in compliance with University policies.

University Networks and Systems for University Business

a. Enterprise-wide University systems and networks, such as but not limited to learning management, email, storage, identity and security services, shall be used for University business. Additionally, University data, records, and research, shall not be stored outside of University information systems. University systems and networks have appropriate security safeguards in place to protect University data, records and research and are managed and administered by University information technology employees. Contracts associated with and for University systems and networks contain provisions that require appropriate technical safeguards and security measures to protect the confidentiality of University records, data, and research and address responsibilities in the event of a data breach. When systems and networks are offered universally across the University by the Information Technology Systems (ITS) department, duplicative systems and networks shall not be provided by other divisions of the University without an approved exception. ITS may be delayed, unable to diagnose, or otherwise unable to provide support in the event of problems with data, records, or research stored in a non-University approved system or network, significantly increasing the risk associated with privacy, data loss, and information security. Examples of the enterprise services that the ITS department will not be able to support include, but are not limited to Drop Box, Google Drive, Survey Monkey and therefore should not be used for storage or collection of University data, records, or research.

b. The university reserves the right to discontinue communication with external systems that are known to harbor spammers, account crackers, or phishing sites, despite the fact that this may restrict certain acceptable communications. When deemed necessary, this action will be taken to protect the security and safety of our systems. Similarly, there may be cases where a particular service or activity on a given university system will, by the very nature of its legitimate operation, tend to generate attacks from other Internet sites. If these attacks are frequent and severe enough to cause service interruptions for larger parts of the campus community, it may be necessary to temporarily or permanently remove these systems from the campus network. In cases where such an action is deemed necessary, network administrators will work with the maintainers of the system to identify alternative methods of network access. In cases where the university restricts access to external sites or removes network access for internal sites, the purpose of the action is to maintain the security and reliability of the computer systems and networks rather than to punish an individual or a site, or to restrict the free expression of ideas.

Security Awareness and Training

All University users accessing University information systems will participate in the University’s security awareness training within thirty (30) days of commencing their employment or affiliation with the University and annually thereafter according to ITS-04: Awareness and Training Standard.

Information Systems Security
ITS provides enterprise-wide endpoint management services that shall be used to securely manage University endpoints and systems to comply with the ITS-02: Risk Classification Standard, ITS-13 Configuration Management Standard Process, and Minimum-Security Controls. Requests for endpoints and systems to not be managed by the provided endpoint management services will be required to submit an exception process in accordance with ITS-01: Policy Exception Standard Process.

a. All University-owned endpoints and systems are to be inventoried and managed by ITS leveraging enterprise-wide endpoint management services in accordance with ITS-13 Configuration Management Standard Process.

b. All University-owned endpoints and systems must enable access control measures such as a password or biometric controls which comply with ITS-07: Access, Identification and Authentication Standard Process.

c. Endpoint device management, inventory software, and antivirus/antimalware software are provided by ITS and are required to be installed and kept up to date on all University-owned endpoints and systems.

d. Endpoints and systems where it is not technically feasible to leverage enterprise- wide endpoint management services shall follow the ITS-02: Risk Classification Standard Process, ITS-13: Configuration Management Standard Process, and ITS-03: Minimum-Security Standard Process.

University networks will be managed by ITS.

Vulnerability Management
All University information systems procured or developed with University resources will be subject to inventory, scanning, and security review in accordance with ITS-10: Risk Management Standard Process. All scanning and security reviews will be conducted under the supervision of the ITS. Information systems are required to meet ITS-13: Configuration Management Standard Process to be allowed to access the network.

Operating System and Application Patch Management
All operating systems and applications must be patched and updated in accordance with ITS-09: System and Informational Integrity Standard Process.

Removable Media/Media Protection
Removable media is intended to facilitate the transfer of data between information systems and not intended for storage or long-term archive in accordance with ITS-12: Removable Media/Media Protection Standard Process. University data and records shall be stored on University information systems as defined in Section 10 of this policy. Removable media can be used to transfer high or medium risk data only if the media or data is encrypted in a manner consistent with the data requirements. Removable media storing University data of any classification are subject to the University data retention policies, procedures, and practices. If removable media is involved in a University e-discovery investigation, the data will be retained, and personnel must ensure that the data destruction process does not destroy any relevant data.

Password Management
Authenticators and authentication strength shall meet or exceed a level of assurance which aligns with the ITS-02: Risk Classification Standard. Two-Factor Authentication, which requires proof of possession and control of two distinct authentication factors, should be used wherever possible.

Information Technology Procurement
University IT equipment, software, and systems will be purchased through the ITS department. ITS will document preferred vendors and negotiate contracts of purchasing with vendors. ITS will define standard purchased endpoints and collaborate with individuals and departments on any customization of devices. This includes equipment, software, and systems purchased with university funds, professional development funds, and grant funds. All equipment, software, and systems purchased with these funds are owned by the university

BYOD Devices
Personally owned computers operating in stand-alone mode or networked through a non-university connection are not covered under this policy, but those users are encouraged to consult the usage policies set forth by their Internet Service Provider.

University employees, agents, affiliates, or workforce members who use personally owned devices for University-related business are responsible for maintaining device security, data return and deletion, incident reporting, response to records requests and discovery requests, and must produce their devices for inspection when required as indicated in ITS-11: Security of Personally Owned Devices

Standard Process.

Only when necessary, for the performance of University-related duties and activities, and after approval of a policy exception, shall high risk data be accessed, transmitted, processed, or stored on personally owned devices, non-University owned cloud services, network attached storage, or removable storage devices (USB drives, memory cards, or similar portable drives and devices). University employees, agents, affiliates, or workforce members shall take all required, reasonable, and prudent actions necessary to ensure the security and retention of high-risk data on personally owned devices. Units shall request on an individual basis whether to allow University employees, agents, affiliates, or workforce members to use personally owned devices to access or maintain high risk data.

Exception Process
The University recognizes that there may be academic or research pursuits that require deviations from these policies, standards, and procedures. Therefore, the University has developed an exception process that users may utilize to justify such deviations and document the associated risks. Exceptions to any portion of this policy require an acceptance of risk and must be jointly approved by the appropriate level of authorization outlined in ITS-01: Policy Exception Standard Process. Approvers for policy exceptions include the President, Provost or Vice President and CIO. Exceptions that have been reviewed and accepted will be documented and maintained by ITS and Risk Management.

Application and Enforcement
This Policy applies to all employees and students of the University. Failure to comply with University IT policies may result in sanctions related to an individual’s use of IT resources.

Inappropriate behavior in the use of computers will be addressed through university policies and related procedures regarding students, faculty, and staff. The offenses mentioned in this policy range from relatively minor to extremely serious, though even a minor offense may lead to more significant consequences if it is repeated or malicious. Certain offenses may also be subject to prosecution under federal, state, or local laws.

The University considers the intent, severity, and history of any incident when determining an appropriate response. Sanctions for offenses will utilize procedures outlined in the Student Code of Conduct, Human Resources policies, or the Faculty Handbook.

Restrictions of Privileges During Investigations
During the course of an investigation of alleged inappropriate or unauthorized use, and after assessing the possible risk to the university or its computing resources, it may be necessary to temporarily suspend a user’s network or computing privileges. This is a precautionary measure and does not imply wrongdoing by the individual involved. For example, if a computer account has been used to launch an attack on another system, that account will be rendered inactive until the investigation is complete. This is a necessary action taken to prevent further misuse and does not presume that the account holder initiated the misuse.

Unsubstantiated reports of abuse will not result in the suspension of accounts or network access unless sufficient evidence is provided to show that inappropriate activity occurred. For example, if someone reports that their computer was “attacked” by a Nebraska Wesleyan system, the burden will be upon the complainant to provide sufficient data logs or other evidence to show that the incident indeed appears to be an attack.

Review and Update
This Policy shall be reviewed and amended by the University's Chief Information Officer at increments no longer than every five (5) years or may be updated periodically for accuracy and clarity based on changes in technology or regulatory requirements.

The NWU Administrative Council approved this policy to be implemented on July 1, 2025. All topics or questions addressed in this policy that occur on or after this date will be subject to this policy and corresponding procedures. This policy supersedes and takes precedence over any prior IT policy or related procedures.
