



Office of Information Technology
2219 SE 68th Avenue
Portland, OR 97215-9988
Phone: (503) 517-1399

Toll Free: 1-800-804-1510 x 1399

Network Access and Acceptable Use Policy

1. Statement of Purpose

Warner Pacific University's computer resources and information network are vital for the fulfillment of the academic, research, and business needs of our community. Their use is provided as a privilege. In order to ensure a reasonable and dependable level of service, it is essential that each individual student, faculty, and staff member exercise responsible, ethical behavior when using these resources. Misuse, even by a few individuals, has the potential to disrupt the legitimate academic work of students and faculty, as well as the business processes of the institution.

The policies that follow outline the principles that govern our academic community in the appropriate use of computer resources and its information network. Unless otherwise stated, these policies apply to all members of the University community and to all University owned or managed computers and network equipment, as well as all information contained therein. Users must abide by all applicable restrictions, whether or not they are built into the operating system or network and whether or not they can be circumvented by technical means.

These policies do not override any existing Warner Pacific University policies as outlined in the Student, Faculty, or Staff Handbooks and are intended to be congruent with all applicable local, state, and federal laws. Use from within the University network by individuals or organizations other than staff, students, or legitimate affiliates is not permitted.

2. Privacy Statement

Warner Pacific University takes reasonable precautions to maintain privacy and security within our electronic systems. However, the University cannot guarantee that these efforts will always be successful. Therefore, users must assume the possibility of breach of University privacy and security systems. The University does not intend to sell, swap, rent, or otherwise disclose for purposes outside the scope of ordinary University functions a user's name, mailing address, telephone number, email address, or other personal information. While the University makes reasonable efforts to protect information provided to us, we cannot guarantee that this information will remain secure and are not responsible for any loss or theft.

Users may not view, use, or otherwise access another person's personal user data unless:

- He or she has such person's consent;
- Such use is necessary to provide technology support services; or
- Such use is necessary, as determined in the sole discretion of the University, to responsibly manage University technology resources or investigate a potential violation of law, University policy, or of this Network Access and Acceptable Use Policy.

The University manages its technology and information resources in compliance with applicable law, including the Family Educational Rights and Privacy Act (FERPA).

3. Copyright Statement

As an institution dedicated to pursuits of the mind, Warner Pacific University recognizes and respects intellectual property rights. Our commitment is to provide an environment that supports the teaching and learning activities of our faculty, staff, and students. To that end, all members of the community are expected to comply with applicable laws regarding copyright and intellectual property and to exercise in good faith the principles of "fair use" in education. The respect of copyright includes all media, including without limitation: print, audio, video, and digital. The University does not permit or support the illegal use or reproduction of copyrighted materials in any form.

Additionally, Warner Pacific University intends to fully comply with all software licenses and takes reasonable steps to assure these intellectual property rights are respected. Users of the University's computers and network resources must comply with all software licenses.

4. Handling of Accounts

The University does not permit the sharing or transfer of passwords or personal identification numbers (PINs) between any individuals. Such action is deemed unacceptable and may result in disciplinary action. If it becomes necessary for an authorized third person to access a user's files or data (as in the case of illness or changing of positions); this must be handled by the system administrator with the permission of the user's supervisor or a member of the Executive Council.

The Office of Information Technology generally removes user accounts, and all data found in user accounts under the following circumstances:

- Upon an employee's termination for any reason (after the employee's supervisor has reviewed the account);
- Upon a student's graduation, leave of absence, withdrawal, or dismissal, and at the end of each academic year;
- Upon a potential student's non-enrollment by the last day of classes in any given semester;
- Upon a post-graduate user's completion of his or her course of study, or upon his or her leave of absence, withdrawal, or dismissal; and
- Upon a legitimate affiliate's termination of affiliation with the University (after the affiliate's sponsor has reviewed the account).

5. Acceptable Use of Computer Resources

Acceptable and responsible use of the University computer and network resources requires that all users follow these guidelines:

- Respect the copyright and license provisions of all programs and data made available on the campus computers and the Internet;
- Respect the copyright of all materials with respect to their incorporation into software, presentations, multimedia applications, and Internet servers;
- Respect the rights of others by not tampering with their accounts, passwords, programs, or data.
- Use only those computer IDs and passwords for which the user is authorized, and use them only for the purposes for which they are intended. Do not share computer accounts or passwords with others;
- Avoid misusing or overusing the network, printing resources, and other shared computing resources;
- Avoid the misuse of University computing and network resources for private, commercial, or political purposes unless such arrangements have been made in advance with the appropriate University official.

Warner Pacific University prohibits unauthorized use or misuse of University email addresses for any purpose, including unauthorized use or misuse of campus electronic mail lists.

All users should respect and preserve the privacy of personal and institutional data to which they may have access by:

- Choosing an obscure or hard password that contains both letters and numbers and changing it frequently;

- Providing security for the computer systems and networks for which they are responsible, including, but not limited to, providing for prevention of unauthorized access or destruction of programs and data, and providing for adequate backups;
- Logging out or securing their workstation when stepping away from a computer to ensure personal account security and to protect the security of our University systems.

6. Unauthorized or Inappropriate Uses

Unauthorized use of technology resources is prohibited and, in many cases, may be a violation of the law. We are guided by the law in noting that unauthorized use includes, but is not limited to, the following types of activities:

- Harassment or threats to individuals or classes of individuals;
- Interference or impairment to the academic activities of others;
- Unauthorized access or unauthorized use of the resources of others;
- Carnage or impairment of University technology resources;
- Unauthorized commercial or political activities;
- Violation of local, state, or federal laws; and
- Anything deemed inappropriate by University policies or regulations, as determined in the sole discretion of the University.

It is the user's responsibility to promptly report any suspected unauthorized or inappropriate use of Warner Pacific University technology resources to the user's supervisor or the Director of Information Technology. Warner Pacific University has the right to investigate such uses, including the inspection of data stored or transmitted on the network or stored on any University owned desktop or laptop computer. If a use is determined to be in violation of this or any other University policy, appropriate measures will be taken which may include, but are not limited to, verbal or written warning, permanent or temporary suspension of user privileges, deletion of files, disconnection from the University's network, referral to the appropriate disciplinary process, and cooperation with appropriate law enforcement officials or agencies.

7. Network and Internet Use

Any computing device that is attached to the Warner Pacific University computer network must comply with the University's security policies, including current Windows patches and updated antivirus software. Since most University computer systems are connected to the Internet, it is essential for each user to recognize his or her responsibility in using these services and systems. The "Internet" is not a single network; rather, it is a group of thousands or individual networks that allow traffic to pass among them. The traffic sent out to the Internet may actually traverse several different networks before it reaches its destination. Therefore, users of the Internet must be sensitive to loads placed on other systems and participating networks.

Each network or system (e.g., accounting, payroll, or the student system) has its own set of policies and procedures. Actions that are routinely allowed on one network or system may be controlled, or even forbidden, on other networks. It is the user's responsibility to abide by the policies and procedures of these other networks/systems.

Access to the network is a privilege that may be revoked at any time, with or without warning, for abusive conduct. Such abusive conduct includes, but is not limited to:

- Using the network for any purpose that violates local, state or federal law;
- Using the network to make unauthorized entry to Warner Pacific University's or other computational information communication resources;
- Use of another person's account on the computer systems;
- Tampering with or moving network cabling or routing devices;
- Use of software or hardware designed to disrupt the security of the network or devices on the network or to spy on the network traffic of other users;
- Knowingly engaging in any activity that spreads computer viruses and/or SPAM mailings to campus computers or other computers on the Internet. This includes users who do not take adequate precautions against, or seek IT support in taking adequate precautions against, viruses and the proliferation of viruses;
- Impersonating another user in the use of the computers, networks or in email or other messages;

- Use of abusive or otherwise objectionable language in either public or private messages;
- Sending of messages that are likely to result in the loss of the recipient's work;
- Sending of "chain letters," novelty messages or lengthy unsolicited messages to individual accounts and/or lists or addresses;
- Distribution of unsolicited advertising and any other types of use that would cause congestion of the networks or otherwise interfere with the work of others;
- Unauthorized use or abuse of University mail lists; and
- Removal of any equipment from its designated location (clusters, labs, classrooms, offices, etc.).

8. Email and Distribution Lists

This policy applies to the University's standard campus email system, which is currently MS Exchange. All members of our campus community are expected to have and regularly check their email accounts. Warner Pacific University email is an official channel of communication between administration, faculty, and students.

While widely used as a primary method of communication between members of our campus community, all users should keep in mind that email is not a secure means of communication. No system connected to the Internet is completely safe from attack or infiltration. Warner Pacific University encourages all members of the community to be cautious in email communications and not send information over email that is highly private, sensitive, or potentially offensive to other members of the community.

Warner Pacific University owns the email system and its contents. Email on this system is not private communication, and users should have no expectation of privacy. Although it may choose to do so, the University does not generally monitor the contents of email sent to or from University servers, except to identify and correct problems with email delivery or receipt, to work with email system problems, or to deal with misconduct or security issues. An electronic log of who sends and receives email through University servers is maintained for a short period of time and used to analyze trends, create summary statistics for internal planning purposes, and to otherwise aid in maintaining system performance and security. Email-related information is generally stored on a temporary basis and released only if required by law or deemed necessary, in the University's sole discretion, to internal investigations of potential violations of University rules, policies or regulations. Lost or deleted email cannot be recovered.

Users should regularly monitor their email storage volume and cull their messages, keeping only those of lasting value or importance.

Due to the importance, purpose, and frequency of email communication, the University wishes to guide students and employees in the use of email distribution lists. This should not be construed as an attempt to prevent communication, but to properly use our technology for the benefit of the institution.

The purpose of email distribution lists is to provide an efficient method to disseminate information directly related to Warner Pacific University activities to multiple relevant recipients. As such, system-wide distribution lists may not be used for non-University communications, including, without limitation, selling, forwarding of jokes, "chain letter" style email messages, remembrances, or medical updates.

In the event the above policy is not followed, a first offense may result in a written warning and a second offense may result in the loss of network privileges.

9. Network Monitoring

The University network is monitored by individuals or software to ensure optimal service. In the event of an outage during non-business hours, users should call extension 1399 and leave a message as to the nature of the outage.

10. Off-Campus Access to Systems and Networks

Only authorized University students, faculty and staff are allowed access to Warner Pacific University systems and networks. Access should be secured by encryption, VPN, gateway authentication, or other necessary means as directed by the Director of Information Technology. Computer-to-computer dial-in access is prohibited.

11. Network Security Policy

Users must comply with any network security policy developed by the Director of Information Technology, including requirements regarding firewalls, filtering, VLAN restrictions, and routing.

12. Bandwidth Usage

The campus network is a resource for the entire University community. Academic use of the network takes priority over recreational use. Users must comply with the University's bandwidth policies and restrictions, which are developed and updated by the Director of Information Technology. These bandwidth policies may include restrictions related to certain Internet activities that may interfere with academic use of the network. These restrictions may include, without limitation, prohibitions on downloads such as:

- MP3 music downloads;
- Video and audio streaming; and
- Online or network gaming.

13. Social Networking

We believe in treating people with respect and adhering to ethical and responsible practices. Employees and students are expected to follow Warner Pacific University's community covenant and lifestyle agreement when representing the University or while on campus, to accept responsibility for the appropriateness of their own conduct, and to show personal integrity at all times.

Electronic media in its various formats is a communication tool used widely among private parties and a growing number of organizations. Warner Pacific University regularly and actively engages the various types of electronic media including, but not limited to: Facebook, LinkedIn, and Twitter as a way to connect to and stay involved with the community at large.

Employees and students are expected to conduct their personal affairs in a manner that is aligned with the University's employment standards and lifestyle agreement and does not adversely affect the University's own integrity, reputation, or credibility. Employees and students should refrain from using electronic media to make inappropriate, unprofessional or adverse comments, suggestions, or innuendo related to or referencing their association with Warner Pacific University. If you identify your association with Warner Pacific in your social networking, the University reserves the right to take issue with texts, posts, or blogging that it deems inappropriate, unprofessional, or adverse. Negative or inappropriate remarks may be injurious to the University, its reputation, and the long-standing position and image built in our community.

Social media references that could be viewed as malicious, obscene, threatening or intimidating, that disparage other employees, students or other campus associates may also be found as a violation of our harassment policy.

Pictures, posts, or texts on a social media or personal site that associate an individual with a violation of the community covenant or lifestyle agreement may serve as a prompt to initiate an investigation into the matter.

Employees found in violation of this policy are subject to disciplinary action up to and including termination. Students found in violation of this policy are subject to disciplinary action up to and including suspension or dismissal from Warner Pacific University. Nothing in this policy should be construed or applied to prohibit employees' rights under the National Labor Relations Act.



Network Access and Acceptable Use Policy Confirmation Statement

The function of Warner Pacific University's communications and data networks is to carry material in support of the academic, business, and research enterprises of the institution. This material may include (but is not limited to) news, electronic mail, and ancillary data relevant to the aims and objectives of the University.

In order to receive an electronic mail account, you must read Warner Pacific University's Network Access and Acceptable Use Policy and complete and sign the form below. Your signature will indicate your willingness to abide by the University's policies.

I have been provided with a current copy of the Warner Pacific University Network Access and Acceptable Use Policy. By signing below, I agree to follow these policy guidelines and understand that failure on my part to do so may result in termination of my electronic mail account and/or other actions as may be specified by this or other Warner Pacific University policies. I also certify that I am either a currently enrolled student attending classes at Warner, or a currently employed faculty or staff member, or a legitimate affiliate of the University. Failure to fill out any information below, including the signature, may result in delay of network access.

Name: _____
(Last) (First) (Middle initial) (Former Last Name)

Contact phone number: (_____) _____ - _____

I am a:

Student --- Student ID #: _____ ADP Cohort: _____

Anticipated Graduation Date (Month and Year): _____

If you are a resident student:

Building Name: _____ Room /APT #: _____ Campus Mailbox #: _____

Faculty/Staff --- Staff ID #: _____ Department: _____

Affiliate/Vendor --- Company (if applicable): _____

Campus Contact Person: _____

Network connection instructions are available at <http://helpdesk.warnerpacific.edu>

Your University email address will be the primary means of distributing University related information to you. Once you receive your default password, you are required to change it. Warner Pacific University does not provide email addresses to individuals or organizations outside of the Warner Pacific University community. Your email address may be included in campus directories.

Signature: _____

Date: _____

For internal use only WSN: _____ UN: _____
--