ELCA Computer and Network Usage Policy **(from the ELCA Student Handbook p. 14 – 18)**

Policy Statement:

Users of the campus network and computer resources have a responsibility not to abuse the network and resources and to respect the rights of others. This policy provides guidelines for the appropriate and inappropriate use of information technologies.

Policy Purpose:

The purpose of the Computer and Network Usage Policy is to ensure an information infrastructure that promotes the basic mission of ELCA. Computers and networks are powerful enabling technologies for accessing and distributing information and knowledge. As such, they are strategic technologies for the current and future needs of the campus. Because these technologies give individuals the ability to access and copy information from remote sources, users must be mindful of the rights of others to their privacy, intellectual property and other rights. This Usage Policy codifies what is considered appropriate usage of computers and networks with respect to the rights of others. With the privileges to use the information resources of these entities come specific responsibilities outlined in this policy.

Summary:

Users of campus information resources must respect software copyrights and licenses, respect the integrity of computer-based information resources, refrain from seeking to gain unauthorized access, and respect the rights of other computer users. This policy covers appropriate use of computers, networks, PODs and other systems and the data and information contained therein.

1. POLICY SCOPE AND APPLICABILITY
    A. Applicability — this policy is applicable to all campus students, faculty and staff and to others granted use of the campus information resources. This policy refers to all campus information resources whether individually controlled or shared, stand-alone or networked. It applies to all computer and computer communication facilities owned, leased, operated, or contracted by either entity of the campus. This includes but is not limited to: word processing equipment, personal computers, workstations, mainframes, minicomputers, PODs (personally owned devices), and all associated peripherals and software, regardless of whether used for administration, research, teaching or other purposes.
    B. Locally Defined and External Conditions of Use - Individual units within the institution may define "conditions of use" for information resources under their control. These statements must be consistent with this overall policy but may provide additional detail, guidelines and/or restrictions. Where such "conditions of use" exist, enforcement mechanisms defined therein shall apply. These individual units are responsible for publicizing both the regulations they establish and their policies concerning the authorized and appropriate use of the equipment for which they are responsible. Where use of external networks is involved, policies governing such use also are applicable and must be adhered to.
    C. Legal Process - The campus does not exist in isolation from other communities and jurisdictions and their laws. Under some circumstances, as a result of investigations, subpoena or lawsuits, either entity of this campus may be required by law to provide electronic or other records, other information related to those records, or relating to use of information resources.
    D. Definitions - Campus - the term campus as used herein refers to Eagle's Landing Christian Academy, Inc. its buildings and grounds, holdings, properties, assets, fixtures and systems both physical and ideological. PODs - Refers to all portable electronic devices that in any way transfer, store , or retrieve data from a campus information system or network.
2. POLICIES

A user of campus information resources who is found to have purposely or recklessly violated any of the following policies will be subject to disciplinary action up to and including, dismissal, expulsion, and/or legal action.

A. Copyrights and Licenses - Computer users must respect copyrights and licenses to software and other on-line information.

1) Copying – All software protected by copyright must not be copied except as specifically stipulated by the owner of the copyright or otherwise permitted by copyright law. Protected software may not be copied

into or from any campus facility or system, except pursuant to a valid license or as otherwise permitted by copyright law.

2) Number of Simultaneous Users - The number and distribution of copies must be handled in such a way that the number of simultaneous users in a department does not exceed the number of original copies purchased by that department, unless otherwise stipulated in the purchase contract.

3) Copyrights - In addition to software, all other copyrighted information (text, images, icons, programs, etc.) retrieved from computer or network resources must be used in conformance with applicable copyright and other law. Copied material must be properly attributed. Plagiarism of computer information is subject to the same sanctions as apply to plagiarism in any other media.

B. Integrity of Information Resources - Computer users must respect the integrity of computer- based information resources.

1) Modification or Removal of Equipment - Computer users must not attempt to modify or remove computer equipment, software, or peripherals that are owned by others without proper authorization.
2) Encroaching on Others Access and Use - Computer users must not encroach on others access and use of campus information systems. This includes but is not limited to: the sending of chain-letters or excessive messages, either locally or off-campus; printing excess copies of documents, files, data, or programs; running grossly inefficient programs when efficient alternatives are known by the user to be available; unauthorized modification of system facilities, operating systems, or disk partitions; attempting to crash or tie up a campus computer or network; and damaging or vandalizing campus computing facilities, equipment, software or computer files.
3) Unauthorized or Destructive Programs - Computer users must not intentionally develop or use programs which disrupt other computer users or which access private or restricted portions of the system and/or damage the software or hardware components of the system. Computer users must ensure that they do not use programs or utilities which interfere with other computer users or which modify normally protected or restricted portions of the system or user accounts. Computer users must not use network links for any use other than permitted in network guidelines. The use of any unauthorized or destructive program may result in legal civil action for damages or other punitive action by any injured party, as well as criminal action.
4) Academic Pursuits - This Institution recognizes the value of research in the educational process and that at times that research may extend outside the boundary of what is acceptable by this policy. Student activity in this area must be under the direct supervision of his /her instructor and must be done with the permission of the Chief Information Officer. The CIO may restrict such activities in order to protect campus and individual computing environments, but in doing so will take account of legitimate academic pursuits.

B. Unauthorized Access — Computer users must refrain from seeking to gain unauthorized access to information resources **or enabling unauthorized access**.

1) Abuse of Computing Privileges - Users of campus information resources must not access computers, computer software, computer data or information, or networks without proper authorization, **or intentionally enable others to do so**, regardless of whether the computer, software, data, information, or network in question is owned by the campus or not. For example, abuse of the networks to which the campus belongs or the computers at other sites connected to those networks will be treated as an abuse of campus computing privileges.

2) Reporting Problems - Any defects discovered in system accounting or system security must be reported to the appropriate administrator so that steps can be taken to investigate and solve the problem.

3) Password Protection - A computer user who has been authorized to use a password- protected account may be subject to both civil and criminal liability if the user discloses the password or otherwise makes the account available to others without permission of the appropriate authority.

C. Usage - Computer users must respect the rights of other computer users. Most campus systems provide mechanisms for the protection of private information from examination by others. Attempts to circumvent these mechanisms in order to gain unauthorized access to the system or to another person's information are a violation of campus policy and may violate applicable law. Authorized administrators may access computer users files at any time for maintenance or security purposes. Administrators will report suspected unlawful or improper activities to the CIO and other authorities as applicable.

1) Unlawful Messages - Use of electronic communication facilities (such as email or chat rooms instant messaging, or systems with similar functions) to send fraudulent, harassing, obscene, threatening, or other

messages that are a violation of applicable federal, state or other law or campus policy is prohibited.

2) Mailing Lists - Users must respect the purpose and charters of computer mailing lists (including local or network news groups and bulletin-boards). The user of an electronic mailing list is responsible for determining the purpose of the list before sending messages to or receiving messages from the list. Subscribers to an electronic mailing list will be viewed as having solicited any material delivered by the list as long as that material is consistent with the list's purpose. Persons sending to a mailing list, any materials which are not consistent with the list's purpose will be viewed as having sent unsolicited material.

3) Advertisements - In general, campus electronic communication facilities should not be used to transmit commercial or personal advertisements, solicitations or promotions.

4) Information Belonging to Others - Users must not intentionally seek or provide information on, obtain copies of, or modify data files, programs, or passwords belonging to other users, without the permission of those other users.

D. Political, Personal and Commercial Use - This institution is a non-profit, tax-exempt organization and, as such, is subject to specific federal, state and local laws regarding sources of income, political activities, use of property and similar matters. It also, at times, may be a contractor with government and other entities and thus must assure proper use of property under its control and allocation of overhead and similar costs.

1) Political Use - Campus information resources must not be used for partisan political activities where prohibited by federal, state or other applicable laws, and may be used for other political activities only when in compliance with federal, state and other laws and in compliance with applicable campus policies.

2) Personal Use - campus information resources should not be used for personal activities not related to appropriate campus functions, except in a purely incidental manner

3) Commercial Use - Campus information resources should not be used for commercial purposes, except in a purely incidental manner or except as permitted under other written policies. Any such commercial use should be properly related to campus activities, take into account proper cost allocations and other overhead determinations and provide for appropriate reimbursement to the appropriate institution for taxes and other costs the entity may incur by reason of the commercial use.

3. ADMINISTRATIVE RESPONSIBILITIES

While Eagle's Landing Christian Academy is the legal "owner" or "operator" of all computers and networks purchased or leased with campus funds, oversight of campus computer and network systems is delegated to the office of the Chief Information Officer, herein also referred to as CIO. Any specific subdivision of the campus governance structure such as a Dean, Department Chair, Administrative or Principal may be delegated as a System Administrator for any particular system or sub-system thereof. This designate has additional responsibilities to the campus as a whole for the system(s) under his oversight, regardless of the policies of his department or group, and the responsible administrator has the ultimate responsibility for the actions of others under his/her authority.

A. The CIO and any designated system administrators should use reasonable efforts:
    1) To take precautions against theft of or damage to the system components.
    2) To faithfully execute all hardware and software licensing agreements applicable to the system.
    3) To treat information about, and information stored by, the system's users in an appropriate manner and to take precautions to protect the security of all systems or networks and the information contained therein.
    4) To promulgate information about specific policies and procedures that govern access to and use of the system, and services provided to the users or explicitly not provided. A written document given to users or messages posted on the computer system itself shall be considered adequate notice.
    5) To cooperate with the system's administrators of other computer systems or networks, whether within or without the campus, to find and correct problems caused on another system by the use of the system under his/her control.
B. Policy Enforcement - Where violations of this policy come to his or her attention, the CIO is authorized to take reasonable actions to implement and enforce the usage and service policies of the system and to provide for security of the system.
C. Suspension of Privileges - The CIO or other system administrators may temporarily suspend access privileges if he or she believes it necessary or appropriate to maintain the integrity of the computer system or network.

D. The CIO or other person designated by this office shall be the primary contact for the interpretation, enforcement and monitoring of this policy and the resolution of problems concerning it. Any issues concerning law shall be referred to the appropriate legal entity for advice.
    1) Policy Interpretation -The CIO or his designee shall be responsible for interpretation of this policy, resolution of problems and conflicts with local policies, and special situations.
    2) Policy Enforcement - Where violations of this policy come to his or her attention, the CIO will work with the appropriate administrative units to obtain compliance. If this fails to bring compliance within a reasonable time period or where abuse or security concerns exist the CIO may take direct action against violators.
    3) Inspection and Monitoring - Only the CIO or designee can authorize the inspection of private data or monitoring of messages (including electronic mail) when there is reasonable cause to suspect improper or illegal use of computer or network resources.

4. CONSEQUENCES OF MISUSE OF COMPUTING PRIVILEGES

A. Cooperation Expected - Users, when requested, are expected to cooperate with CIO in any investigation of system abuse. Users are encouraged to report suspected abuse, especially any damage to or problems with their files. Failure to cooperate may be grounds for cancellation of access privileges, or other disciplinary actions.
B. Corrective Action - If a designated system administrator should have persuasive evidence of misuse of computing resources, and if that evidence points to the computing activities or the computer files of an individual, they should pursue one or more of the following steps, as appropriate to protect other users, networks and the computer system.
    1) Provide notification to the CIO and to the appropriate entity's administrative head, as well as the user's instructor, department or division chair, or supervisor if applicable.
    2) Temporarily suspend or restrict the user's computing privileges during the investigation. A student may appeal such a suspension or restriction and petition for reinstatement of computing privileges through the appropriate entity's administrative head. Staff and faculty members may appeal through applicable dispute resolution procedures.
    3) Inspect the user's files and/or other computer-accessible storage media.
    4) Refer the matter for possible disciplinary action to the appropriate authority.
C. Legal Compliance - In cases involving a violation of statutory law; the facts, circumstances, and applicable evidence may also be referred to the appropriate law enforcement agency for possible judicial remedy as well.

5. STUDENT HONOR CODE AND FUNDAMENTAL STANDARD

Unless specifically authorized by a class instructor, all of the following uses of a computer are examples of possible violations of the Honor Code:

A. Copying a computer file that contains another student's assignment and submitting it for credit;
B. Copying a computer file that contains another student's assignment and using it as a model for one's own work;
C. Collaborating on an assignment, sharing the computer files and submitting the shared file, or a modification thereof, as one's individual work. In addition, student misuse of a computer, network or system may violate the Fundamental Standard. Examples would be, but are not limited to: theft or other abuse of computer time, including unauthorized entry into a file, to use, read, or change the contents; unauthorized use of another person's identification or password; use of computing facilities to send abusive messages; or use of computing facilities to interfere with the work of another student or the work of a faculty or staff member. For cases involving a student, referring the case to the student's principal is the recommended course of action. This ensures that similar offenses may be considered for similar punishments, from quarter to quarter, year to year, and instructor to instructor. It also allows the detection of repeat offenders.