

STUDENT COMPUTER NETWORK RULES AND APPROPRIATE USE POLICY

CALIFORNIA WESTERN SCHOOL OF LAW Student Network (“CWSLSN”)

1. The 290 Collaborative Space may be reserved by faculty or library staff at any time for training purposes. Every effort will be made to notify students in advance of these training sessions.

APPROPRIATE USE OF NETWORK & COMPUTERS:

Note: the term 'network' used in this document includes all CWSL wired and wireless networks.

1. **Introduction:** The purpose of this document is to provide guidelines for the responsible use of computing, and for maintaining the integrity of the cabled and wireless networking systems at CWSL. Student use of CWSL computer and network resources is governed by this policy, the CWSL Student Honor Code, and applicable state and federal laws.

2. **Access:** The computer resources and facilities are solely for the use of CWSL registered students, faculty, staff, and approved guest accounts.

3. **Confidentiality & Ownership:** We will attempt to ensure the security of information residing on CWSL computing systems. Computing systems encompass all computer related equipment including but not limited to hardware, software, cabling, phone lines, data and communication devices that are CWSL property or under its control. The information residing on CWSL computing systems is considered proprietary in nature and is there to be viewed, accessed and disseminated only by or to authorized persons. Information residing on all CWSL computer systems is CWSL property. CWSL does not guarantee the privacy of data or use and reserves the right to monitor files, e-mail, and any usage of computer resources.

4. **Violations:** Violation of this policy, or applicable state and/or federal laws, may result in a permanent loss of computing privileges, referral to the proper authority on campus, administrative action, probation, suspension, expulsion, an obligation to make financial restitution, a fine and/or imprisonment. Violations of any computer system, computer laws and policies, and/or breach in security of any computer equipment should be reported as follows:

**** Within the Library:** Report violations to the Library’s Associate Director for Public Services & Educational Technology, who will notify the Library Director and the Executive Director of Enterprise Systems when appropriate. The Executive Director of Enterprise Systems or the Library Director will notify the Vice Dean and/or Dean of Students, who will notify the Honor Code Violations Committee when a student is involved, or the Dean, when a non-student is involved.

**** Outside the Library:** Report violations to the Executive Director of Enterprise Systems, who will then follow the appropriate procedures stated in the previous paragraph. The user community is expected to cooperate with CWSL in its operation of computer systems and networks as well as in the investigation of misuse or abuse. Should the security of a computer system be threatened, user files may be examined under the direction of the appropriate Law School officials.

5. **It is a violation of CWSL appropriate use policy for an individual to do any of the following:**

- a. Create an unauthorized "Rogue" network connected to any CWSL network or computer.
- b. Use any of the microcomputers, workstations or networks for other than CWSL-related course work, research project or departmental activity. Computers, workstations or networks must not be used for individual personal financial gain unless in support of CWSL research or department projects or as permitted by CWSL policies.
- c. Use a network account that was not assigned to you by CWSL as a single or multiple-access user.
- d. Provide a password that was assigned to you by CWSL as a single or multiple-access user to another individual.
- e. Attempt to disguise the identity of the account or machine you are using.
- f. Attempt to circumvent data protection schemes or uncover security loopholes.
- g. Deliberately perform an act which will seriously impact the operation of computers, terminals, peripherals or networks, including but not limited to theft of equipment, tampering with the components of a local area network (LAN) or the high-speed backbone network, otherwise blocking communication lines, or interfering with the operational readiness of a computer.
- h. Run or install on any of the computer systems, or give to another, a program which could result in eventual damage to a file or computer system and/or the reproduction of itself. This is directed toward but not limited to the classes of programs known as Malicious Software.
- i. Attempt to modify in any way hardware or software which CWSL supplies for any type of use at its sites. It is also a violation to load personal software onto the computer system without the express written permission of the Executive Director of Enterprise Systems or the Library's Associate Director for Educational Technology and Strategic Initiatives.
- j. Deliberately perform acts which waste computing resources. These acts include but are not limited to sending mass mailing or chain letters, obtaining unnecessary output, creating unnecessary multiple jobs or processes, or creating unnecessary network traffic.
- k. Harass others by sending annoying, threatening, libelous, or sexually, racially or religiously offensive messages.
- l. Attempt to monitor another user's communications, or read, copy, change or delete another user's files or software, including e-mail and voice mail, without the owner's permission.
- m. Intercept or interfere with the printing or downloading of the data of another user.
- n. Fail to abide by the terms of all software licensing agreements and copyright laws.
- o. Place the following information or software on any CWSL-owned system on or off campus:
 1. That which infringes upon the rights of another person.
 2. That which is abusive, profane or sexually offensive to the average person.
 3. That which consists of information which may injure someone else and/or lead to a lawsuit or criminal charges. Examples of these are pirated software, destructive software, obscene materials or libelous statements.
 4. That which consists of any advertisement for commercial enterprises.

In addition, CWSL reserves the right to monitor all network bandwidth and/or prohibit any traffic that interferes with legitimate use of network resources. CWSL will manage the voice, data and video bandwidth. Prohibited activities include but are not limited to use of a computer or any device to monopolize network bandwidth and interfering with access to Internet based resources. The unauthorized sharing of any material not authored or created by the sender over the network

is prohibited. This includes but is not limited to copyrighted materials, classroom lectures or other intellectual property. For example: movies, music or audio or video recordings of classroom lectures.

6. Digital Millennium Copyright Act

The Digital Millennium Copyright Act provides certain liability protections for online service providers, including CWSL, when their computer systems or networks carry materials that violate (infringe) copyright law. To qualify for liability protection, our law school is required to have a policy under which the computer accounts of users will be terminated if they repeatedly infringe on the copyrighted works of others.

Policy Statement:

Students, faculty and staff at CWSL are expected to comply with federal copyright law. Most creative and intellectual work has copyright protection even if it does not explicitly indicate it is copyrighted. Most often copyright is held by the author, but this may not necessarily be the case. Text (including email and web information), graphics, art, photographs, music, and software are examples of types of work protected by copyright.

*** Copying, saving, distributing, sharing, downloading, and uploading a copyrighted work on the Internet, even if innocent or unintentional, may infringe the copyright for that work. Whenever CWSL becomes aware of probable violations of copyright law, the school will investigate and take timely action to stop such infringement. In the case of repeat infractions by a single network user, such action may include terminating the user's computer account and other access privileges.*

*** CWSL personnel will periodically scan user's network storage space for possible illegal copies of copyrighted files and require user to delete these files or show proof of valid license. Students who continually store illegal copies of copyrighted files on CWSL network storage space may lose network privileges. Note: This does not apply to student data NOT stored on the CWSL network.*

7. Use of the network during classroom teaching is subject to any additional restrictions imposed by the instructor.