Appropriate Use of Computers for Faculty & Staff

Updated December 2019

(1) **Introduction** This policy is to provide guidelines for the responsible use of computing, networking and message systems at California Western School of Law (the "Law School"). It is intended to augment existing laws and policies on this issue. Use of the computer resources is governed by this policy and applicable state and federal laws.

(2) **Access** The computer resources are solely for use by registered students, faculty, staff and approved guest accounts.

(3) **Confidentiality** Every attempt must be made to ensure the security and confidentiality of the information residing on the computing systems. Computing systems encompass all computer related equipment including but not limited to hardware, software, cabling, phone lines and communication devices that are on Law School property. The information residing on the Law School computing systems is considered proprietary in nature and is therefore to be viewed, accessed and disseminated only by or to authorized persons. Information about individuals should be on a need-to-know basis only.

(4) **Electronic Mail (e-mail) & Voice Mail (v-mail)** The Law School permits employees to receive, send, and transfer messages via its computer and telephone systems. These systems are assets of the Law School installed to facilitate business communications. Although employees may use codes to restrict access to messaging systems, the systems are intended solely for business use. The Law School reserves the right to monitor, gain access, restrict access, and examine the contents of both electronic and voice mailboxes.

(5) **Violations** Violation of this policy, or state and/or federal laws can result in a permanent loss of computing privileges, referral to the proper authority on campus, administrative action, probation, suspension, termination, requirements to make financial restitution, a fine and/or imprisonment. For violations of any computer system, computer laws and policies, and/or breach in security of any computer equipment within the Law School, the Executive Director of Enterprise Systems is to be notified, who, when appropriate, will notify the Cabinet. The user community is expected to cooperate with Information Technology in its operation of computer systems and networks as well as in the investigation of misuse or abuse. Should any system's security be threatened, user files may be examined under the direction of the appropriate Law School officials. It is a violation of this policy to do any of the following:

- Use a computer ID without permission that was not assigned to you as a single or multiple access user by Information Technology.
- Attempt to disguise the identity of an account or machine.
- Attempt to circumvent data protection schemes or uncover security loopholes
- Deliberately perform an act which will seriously impact the operation of computers, terminals, peripherals or networks, including but not limited to 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.

(6) Run or install on any of the computer systems, or give to another, a program which could result in the 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 computer viruses, Trojan Horses and worms.

(7) Attempt to modify in any way hardware or software which Information Technology supplies for any type of use at its sites

(8) Deliberately perform acts that are wasteful of computing resources. These acts include, but are not limited to:

- sending mass numbers of unauthorized emails

- generating unnecessary or unauthorized print output
- creating unnecessary network traffic (for example, by using unauthorized file sharing or peer-to-peer software).

(9) Harass others by sending annoying, threatening, libelous, or sexually, racially or religiously offensive messages.

(10) Attempt to monitor another user's communications, or read, copy, change or delete another user's files or software, without permission.

(11) Fail to abide by the terms of all software licensing agreements and copyright laws.

(12) Place the following information on any Law School owned system

- That which infringes upon the rights of another person.
- That which is abusive, profane or sexually offensive to the average person.
- That which may injure someone else and/or lead to a lawsuit or criminal charges. Examples are pirated or destructive software, obscene materials or libelous statements..
- That which consists of any solicitation or advertisement for commercial enterprises.
- Personal files, unrelated to Law School business, included but not limited to music, photo, audio or video files. The school could be held liable for copyright infringement.

(13) 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.

(14) Students, faculty and staff at the Law School 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 the Law School 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 temporarily disabling the user's computer account and other access privileges, or termination of the user.
- Law School personnel may periodically scan any and all network storage space for possible illegal copies of copyrighted files and require user to delete these files or show proof of valid license. Personnel who continually store illegal copies of copyrighted files on Law School network storage space may lose network privileges.