

# Computer Usage

In support of its mission of teaching, scholarship, and service, the School of Law provides computer access for students. The computing resources of the School of Law, including computers, facilities, hardware, software, networks, and computer accounts, are the property of the School of Law. The use of these resources is a privilege granted by the School of Law to authorized users only. The School of Law requires all persons authorized to use its computing resources to do so responsibly and in compliance with all state and federal laws, all contractual and license agreements, and all policies of the University and the School of Law. Authorized users of the School of Law's computing resources must act responsibly to maintain the integrity and security of these resources. Each user of the School of Law's computing resources is ultimately responsible for the use of that computing resource and for the use of his or her computer account. Persons misusing the School of Law's computing resources in violation of federal and state laws or policies promulgated by the University or the School of Law are subject to disciplinary actions by the School of Law and/or forfeiture of their computer privileges. In the event such misuse of computer resources threatens to compromise the integrity or jeopardize the security of university computer resources or harm authorized users of those resources, the University's Chief Information Officer, the Dean, or any of their designees is authorized to take any and all necessary actions, including the immediate confiscation and/or disabling of a university computer resource or the temporary or permanent termination of a computer account, to protect, investigate, and ensure the security and proper use of computer resources.

1. Use of any School of Law computing resource is restricted to those having proper authorization to use that particular resource. It is a violation of the law and School of Law policy to assist in, encourage, or conceal from authorities any unauthorized use, or attempt an unauthorized use, of any of the School of Law's computers or network facilities.
2. No one shall knowingly endanger the security of any School of Law computing resource nor willfully interfere with authorized computer usage by circumventing or attempting to circumvent normal resource limits, logon procedures, or security regulations.
3. No technologies shall be connected to the School of Law's computing resources that interfere with authorized usage of those resources. The School of Law reserves the right to restrict the use of any technologies that may endanger the security and/or integrity of its computing resources.
4. The School of Law's computing resources shall not be used to attempt unauthorized use, or to interfere with another person's legitimate use, of any computer or network facility anywhere. Encroaching on, or disrupting another person's use of, the School of Law's computers is prohibited. Examples of such acts include but are not limited to: sending excessive messages either locally or off campus [including but not limited to electronic chain letters]; initiating denial of service attacks; printing excessive copies of documents, files, data, or programs; modifying system facilities, operating systems, or disk partitions; attempting to crash or tie up a university computer; damaging or vandalizing university computing facilities, equipment, software, or computer files; causing an inordinately large number of requests for files; spamming; sniffing; running scans; reconfiguring; or using an inordinately high percentage of bandwidth.
5. University computing resources and network facilities shall not be used for commercial purposes without specific authorization from the Dean or his or her duly authorized designee.
6. Passwords to any computing resource shall only be issued to authorized users. Password recipients are responsible for the integrity of their password and shall not distribute it to unauthorized users.
7. Misrepresenting a person's identity or relationship to the School of Law when obtaining or using School of Law computer or network privileges is prohibited.
8. Accessing, reading, altering, or deleting any other person's computer files or electronic mail without specific authorization is prohibited.
9. Copying, installing, distributing, infringing, or otherwise using any software, data files, images, text, or other materials in violation of copyrights, trademarks, service marks, patents, other intellectual property rights, contracts, or license agreements is prohibited. All usage of computing resources shall be in compliance with federal and state copyright laws.
10. Creating, installing, or knowingly distributing a computer virus, "Trojan horse," or other surreptitiously destructive program on any School of Law computer or network facility, regardless of whether any demonstrable harm results, is prohibited.
11. Only those persons with proper authorization shall modify or reconfigure any School of Law computing resource or network facility.

12. Users of the School of Law computing resources shall have no expectation of privacy for materials downloaded, used, viewed, or stored on those resources. The School of Law reserves the right to access any of its computer resources AT ANY TIME FOR ANY REASON OR FOR NO REASON, WITH OR WITHOUT NOTICE. Furthermore, the School of Law makes no representation or guarantee that information transmitted on its network will not or cannot be accessed by third parties. By using the School of Law's computer resources, students release and hold the University and the School of Law harmless for any unauthorized access to information transmitted.
13. Authorized computer users shall take full responsibility for messages that they transmit through the School of Law's computing resources. The School of Law's computing resources shall not be used to transmit any communications prohibited by law, including but not limited to fraudulent, harassing, obscene, or threatening messages.
14. Students are prohibited from downloading any software programs on law-school issued computers without express, written permission from the associate dean for academic affairs.
15. The University's training option for all Microsoft Office products (and many more software products), and Linked in Learning is available to students, faculty, and staff.

Violation of any rule contained within this section shall constitute a sufficient basis for disciplinary action(s) by the university and/or the school of law. Additionally, violations of any rule contained within this section shall constitute a violation of the code of academic integrity.