SOUTHWESTERN
LAW SCHOOL
Los Angeles, CA

Computer and Network Use Policy

Administrative policy approved January 18, 2022. Effective immediately.

Revision history: Administrative review and technical edits performed on January 10, 2022; clean-up edits in May 2023; revised November 2023 to expressly identify doxxing.

Related policies: Peer-to-Peer File Sharing Policy; Policy to Prevent Discrimination, Harassment, and Retaliation

Scheduled Review Date: August 2024 (Information Technology)

A. Policy Statement

This policy governs the use of computer, communication, and network resources at Southwestern Law School. Use of any of these Southwestern resources constitutes acceptance of this policy.

B. Acceptable Uses

Southwestern computing resources are provided to support the instructional, research, and administrative activities of Southwestern. Resources should not be used for personal or private activities not related to appropriate Southwestern functions, except in an incidental manner. Access to computing resources is a privilege. Southwestern may revoke this privilege without notice or take other disciplinary action against any individual who fails to comply with this policy.

C. Prohibited Conduct

Activities that violate this policy include, but are not limited to:

1. any use that violates local, state, or federal law;
2. any use that violates any policy, procedure, or rule contained in Southwestern's Employee Handbook, Faculty Manual, or posted on Southwestern's Institutional Policies webpage;
3. using the Southwestern network to gain unauthorized access to any computer system;
4. connecting unauthorized equipment to the Southwestern network or network component;

5. attempting to circumvent data protection schemes or uncover security, which includes creating or running programs that are designed to identify security loopholes or decrypt intentionally secure data;
6. performing an act that will interfere with the normal operation of computers, terminals, peripherals, or networks;
7. running or installing on any computer or network any program intended to damage, interfere with, or place excessive load on the computer system or network; this provision includes, but is not limited to, programs known as "malware," "computer viruses," "Trojan Horses," and "worms";
8. violating terms of applicable software licensing agreements or copyright laws;
9. violating copyright laws and their fair use provisions through inappropriate reproduction of copyrighted text, music, images, etc., including through illegal or inappropriate Peer-to-Peer (P2P) file sharing (see Peer-to-Peer File Sharing Policy);
10. using Southwestern resources for any commercial activity or personal financial gain;
11. using electronic mail to harass or threaten others, which includes sending repeated, unwanted e-mails to others (the term "others" includes Southwestern students, faculty, staff, and persons not registered at, affiliated with, or employed by Southwestern);
12. initiating or propagating electronic chain letters;
13. initiating mass mailings not authorized by an authorized Southwestern official; "mass mailings" includes multiple mailings to newsgroups, mailing lists, or individuals (e.g. "spamming," "flooding," or "phishing");
14. forging the identity of another person or machine in an electronic communication;
15. transmitting or reproducing materials that are defamatory in nature;
16. creating an intimidating, hostile, or offensive educational environment by displaying images or text where it can be viewed by others with the intent, or having the effect, of unreasonably interfering with another's educational or work performance. Southwestern computing facilities may not be used as instruments for harassment as defined in Southwestern's Policy to Prevent Discrimination, Harassment, and Retaliation;
17. doxxing, which involves revealing online, emailing, or electronically publishing or distributing another person's personal information, including but not limited to their home address, phone number, financial information, or other personal information, without their permission and with (a) the intent to place that person in reasonable fear for their own safety or their family's safety, (b) the purpose of imminently causing the person or their family unwanted physical contact, injury, or harassment, or (c) the intent to incite unlawful actions;
18. attempting to monitor or tamper with another's electronic communications, or reading, copying, changing, or deleting another's files or software without the explicit agreement of the owner;
19. disclosing your password to another person or permitting another person to use your account;
20. using the Southwestern name, logo, or copyrights in a way that suggests or implies institutional authorization or endorsement.

D. Sanctions

Computing staff, in consultation with the Chief Information Officer, Vice Dean, or the Associate Dean for Library Services when practicable, are authorized to suspend or modify, without notice, network access for actual or suspected violations of this policy. Actions may include, without limitation, halting a program running on Southwestern equipment; disconnecting remote systems from the network; removing offending files from the system or rendering them inaccessible; and disabling user accounts.

Once services have been suspended or modified, the matter may be referred for further action to the appropriate office, including the Office of the Dean, the Administrative Services Office, or the Student Services Office. Violations of this policy may result in the loss of computing privileges or disciplinary action up to and including termination or expulsion from Southwestern. Activity that is illegal under local, state, or federal law may be referred to the appropriate law enforcement authorities.

E. Privacy and Confidentiality

Southwestern reserves the right to monitor, inspect, and examine any Southwestern-owned or -operated communication system, computing resource, file, or information contained therein at any time.

If inspection or examination of any Southwestern-owned or -operated communication system, computing resource, file, or information contained therein is requested by a source outside Southwestern, Southwestern will treat the information as confidential unless:

1. authorized by the owner of the information, by the Dean, or the Dean's designee to release the information;
2. required by local, state, or federal law to release the information;
3. required by a valid subpoena or court order to release the information.

F. Disclaimer

Although Southwestern attempts to maintain an error-free hardware and software environment and to properly train computing staff, it is impossible to ensure that hardware or system software errors will not occur, or that staff will always give correct advice. Southwestern makes no warranty, either express or implied, for the services provided. Damages or loss resulting directly or indirectly from the use of these resources are the sole responsibility of the user.

G. Policy Revisions

Southwestern reserves the right to change or modify any aspect of this policy at any time, with or without notice.