**Administrative Guidelines**

**Acceptable Use of Network Resources**

**Overview**

This policy provides guidelines for, and promotes, the responsible and ethical use of the shared computing resources of Southern Wesleyan University. It is in the best interests of the community as a whole that computing resources be used in a manner which protects the equipment and the rights of all users. This policy covers students, faculty, staff, outside agents, contractors, and any and all individuals or entities using any Southern Wesleyan University IT Resources and all uses of such IT Resources University-wide.

Those responsible for campus computing facilities not administered by Information Technology, such as those in the library, may have additional regulations consistent with this policy to control their use. System administrators are responsible for publicizing any additional regulations concerning the authorized and appropriate use of the equipment for which they are responsible.

**General Rules**

As in all aspects of life, a user of computing facilities should act in a manner consistent with ordinary interpersonal and ethical obligations. Cheating, stealing, making false or deceiving statements, plagiarism, vandalism, and harassment are just as wrong when done in the context of computing as they are in all other aspects of conduct. Individuals should use only those computing facilities they have been authorized through ordinary channels to use.

**Acceptable use**

Use resources only for authorized purposes. Protect your user id and system from unauthorized use. You are responsible for all activities on your user id or that originate from your system. Your user id and password act together as your electronic signature. Access only information that is your own, that is publicly available, or to which you have been given authorized access. Use only legal versions of copyrighted software in compliance with vendor license requirements. Be considerate in your use of shared resources. Refrain from monopolizing systems, overloading networks with excessive data, degrading services or wasting computer time, connection time, disk space, printer paper, manuals, or other resources.

**Unacceptable Use**

Use another person's system, files, or data without permission (note that permission from an individual user may not be sufficient. Some systems may require additional authority). Give your password to another person. Contact the IT [Help Desk](http://www.swu.edu/IT/helpdesk.htm) if you need assistance with giving other people authority to access your files or e-mail. Use computer programs to decode passwords or access-controlled information. Attempt to circumvent or subvert system or network security measures. Engage in any activity that might be purposefully harmful to systems or to any stored information. For example, do not create or propagate viruses, worms, or "Trojan horse" programs, or disrupt services, damage files, or make unauthorized modifications to university data. Make or use illegal copies of copyrighted software, store such copies on university systems, or transmit them over university networks. Use mail or messaging services to harass or intimidate another person, for example, by broadcasting unsolicited messages, by repeatedly sending unwanted mail, or by using someone else's name or user id. Waste shared computing or network resources, for example, by intentionally placing a program in an endless loop, by printing excessive amounts of paper, or by sending chain letters or unsolicited mass mailings. Use the university's systems or networks for commercial purposes, for example, by selling access to your user id or by performing work for profit with university resources in a manner not authorized by the university. Use the university’s computers or your personal computer to view inappropriate material (pornography) as outlined in the student handbook. Enter any computer lab with drink or food.

**Terms and Conditions**

Reasonable suspicion of a violation of the principles or practices described in this policy statement may result in disciplinary action. Such action will be taken through appropriate Southern Wesleyan University channels such as administrative procedures, the Honor Council, or other supervisory authority to which the individual is subject. Violation of local, State, or Federal statutes may result in civil or criminal proceedings.

With due regard for the right of privacy of users and the confidentiality of their data, system administrators have the right to suspend or modify computer access privileges, examine files, passwords, accounting information, printouts, tapes, and any other material that may aid in maintaining the integrity and efficient operation of the system. Users whose activity is viewed as a threat to the operation of a computing system, who abuse the rights of other users, or who refuse to cease improper behavior may have, at the very least, their user privileges revoked. In the event that access to a system is revoked, users will be provided a copy of their files upon request.

**Responsibility**

The Director of Information Technology has responsibility for the administration of this policy. Issues of interpretation and enforcement of this policy shall be resolved by the director and may include participation from appropriate academic or administrative officials or committees as deemed necessary by the Director of Information Technology.