Southern Adventist University

Employee Computer and Internet Policy

Version 2.0 - Revised Aug 20 2018

Scope

This policy governs the employees' use of computer and Internet resources at Southern Adventist University. This augments Southern's Acceptable Use Policy.

Legitimate Use

Southern Adventist University electronic systems, including computers, fax machines, and all forms of Internet or network access, must always be used for purposes consistent with the university principles and are intended primarily for university business.

Ownership of information

The university owns the rights to all data and files in any university-owned computer or storage device. In the case of scholarly work or other intellectual property produced at Southern, the copyright ownership is decided according to the guidelines contained in Southern's Intellectual Property Policy.

In order to assure compliance with university policies and state and federal laws, the university has the right to inspect any file stored on individual computers or storage media connected to university secure networks.

Internet Browsing

The Internet is to be used to further the university's mission, to provide effective service of the highest quality to the university's faculty and staff, and to support other direct job-related purposes. Supervisors should work with employees to determine the appropriateness of using the Internet for professional activities and career development.

Employees should assume that whatever they do, type, enter, send, receive, and view on university electronic information systems could be electronically stored and could be subject to inspection, monitoring, evaluation, and university use at any time as defined in the Southern Information Security Policy. There should be no expectation of privacy in any activity conducted, sent, performed, or viewed on or with university equipment or Internet access.

Personal Equipment & Cloud Services

Due to the significant risk of harm to the university's electronic resources, or loss of data from any unauthorized access that causes data loss or disruption, employees should not use personal devices or personal cloud storage services in the workplace while connected to the university network zones that have access to Sensitive or Confidential Data (as defined in the Data Classification Policy) unless expressly permitted to do so by Information Technology.

User Responsibility

Use of university computers, networks, and Internet access is a privilege. Engaging in certain activities is prohibited and may cause your access to be revoked. Such activities include but are not limited to:

- Participating in any way in the creation or transmission of unsolicited commercial e-mail ("spam") that is unrelated to legitimate university purposes;
- Automatic forwarding of Southern email to email systems outside of Southern;
- Accessing networks, servers, devices, drives, folders, or files to which the employee has not been granted proper access;
- Making unauthorized copies of university files or other university data;
- Maliciously destroying or concealing university files or other university data, or otherwise making such files or data unavailable or inaccessible to the university or to other authorized users of university systems;
- Misrepresenting oneself or the university;
- Violating the laws and regulations of the United States;
- Deliberately propagating any virus, worm, Trojan horse, trap-door program code, or other code or file designed to disrupt, disable, impair, or otherwise harm either the university's networks or systems or those of any other individual or entity;
- Intentionally sending or accessing inappropriate materials as defined by university policies;
- Causing congestion, disruption, disablement, alteration, or impairment of university networks or systems;
- Defeating or attempting to defeat security restrictions on university systems and applications.

Violations

Violation of this policy, or failure to permit an inspection of any device under the circumstances covered by this policy, may result in disciplinary action, up to and possibly including immediate termination of employment, depending upon the severity and repeat nature of the offense. In addition, the employee may face both civil and criminal liability.