

Mitchell College Library and Information Technology Services Information Systems Appropriate Use Policy

The policy outlined herein applies to all Mitchell College (“College”) Information Systems users, whether or not they have permission to use the College Information Systems.

Definitions

Mitchell College Information Systems refers to all information technology resources including but not limited to computers, networks, network user accounts, servers, printers, software, phone and voicemail systems, electronic mail, and web pages developed, maintained and/or managed by the College and/or its affiliates.

Mitchell College User refers to any College student, faculty, staff, or affiliate using the College Information Systems.

Mitchell College Domain Administrator refers to any individual with express permission and authority from the College to administer and facilitate access to the College Information Systems.

Mitchell College User Account refers to any account assigned by a College Domain Administrator to faculty, student, staff, or affiliate. A user who has been assigned a user account has permission to use the College Information Systems within the parameters determined by the Domain Administrator, this Appropriate Use policy, and other College policies and regulations.

Principal of Least Privilege (PoLP) is a basic security guideline stating that “every program and every user of the system should operate using the least set of privileges necessary to complete the job.”¹

Purpose of this Policy

The purpose of this policy is to outline the College users’ rights and responsibilities regarding appropriate use of the College Information Systems. This policy is not intended to cover every situation, but instead to provide general guidelines for all users.

Restrictions

The College reserves the right to protect its Information Systems and to restrict user access to Information System activities that are related to the College. These systems are primarily intended for the academic, educational, and research purposes of the College. The College reserves the right to define what constitutes unauthorized use.

The College and its users must comply with relevant federal and state laws, including but not limited to, appropriate use, copyright and fair use, and privacy laws.

Network User Accounts

To utilize the Mitchell College network, the College requires all users to log on with the accounts that have been provided to them by a Domain Administrator. Users are strictly prohibited from sharing user account information with others or using someone else’s user account, with or without their permission. Any users suspecting unauthorized use of their

accounts are responsible for changing their passwords and/or contacting a Domain Administrator through the help desk to have their accounts temporarily or permanently disabled.

Mitchell Email

An email account is automatically provided with each user account. Requests to forward Mitchell College email accounts to outside email accounts will be denied.

Appropriate Use of Information Systems

Users are responsible for using the College Information Systems in an efficient, ethical, and lawful manner. Usage that conflicts with this policy is prohibited, and includes, but is not limited to, the following:

- Supporting commercial interests not related to the work of the College.
- Initiating or propagating electronic chain mail, commercial mailings, or other mass mailings in violation of the CAN-SPAM Act of 2003.
- Intentionally introducing viruses, worms, Trojan horses or other malicious activity.
- Engaging in any activity that interferes with the proper operation of the College Information Systems.
- Installing software on College computers without the authorization of a Domain Administrator.
- Tampering or interfering with the intended use of the College Information Systems.
- Engaging in any unauthorized activities that result in monetary charges to the College.
- Using the College Information Systems to convey fraudulent, defamatory, harassing, obscene, or threatening messages or material and/or any communications prohibited by law.
- Using the College Information Systems to engage in illegal file sharing or any other illegal activities.

Non-commercial, Personal Use

Mitchell College acknowledges that users of the College Information Systems may engage in non-commercial, personal use (e.g. personal email). Such use is permitted within the following guidelines:

- Use does not interfere with the performance of any user's college-related responsibilities.
- Use does not interfere with the performance of the College Information Systems.
- Use is not otherwise prohibited by this policy, by other College policies, or by law.

Administrative Privileges

Mitchell College assigns administrative privileges based on the Principle of Least Privilege (PoLP). Individual users may be assigned administrative privileges on a case-by-case, temporary basis by submitting a request through the help desk. The help desk will process the request through the appropriate channels as necessary, i.e. the Domain Administrator, the Director of Information Services, and/or the Chief Information Officer.

Harassment

The College has set forth explicit policies in the student and faculty/staff handbooks regarding harassment. Harassment within the context of the College Information Systems is prohibited and all incidents will be dealt with appropriately.

Privacy

The College acknowledges its responsibility – pursuant to this policy, the *Family Educational Rights & Privacy Act (FERPA)*, the *USA Patriot Act of 2001*, *U.S. Privacy Act*, and the *Electronic Communications Privacy Act (ECPA)* – to respect the privacy of students' electronic files and communications within the College Information Systems. However, users of these Information Systems should be aware of the inherent limitations of shared information system resources. The College cannot guarantee the privacy or confidentiality of stored information or electronic communications.

At all times, the College has the right to monitor and access a user's communications, files, stored information, and activities using the College Information Systems pursuant to state and federal law and College policies.

If the College monitors or accesses a user's files, communications, or activities using the College Information Systems, it will respect that which is privileged or otherwise protected from disclosure by law.

Sanctions

Violation of these policies may result in the temporary or permanent disabling of the user account, depending on the severity of the offense. Other sanctions, up to and including dismissal and/or termination and prosecution under state and federal law, may apply.

Statement regarding sources for the above: This draft was assembled using policy statements from MIT, Connecticut College, Eastern Connecticut State University, Central Connecticut State University, Pennsylvania State University, Trinity College, Trinity University, Wesleyan University, and University of Connecticut.

¹ SALTZER, J.H. AND SCHROEDER, M.D., 'The Protection of information in computer systems,' Proceedings of the IEEE, vol. 63, no. 9 (Sept 1975), pp. 1278-1308.