

(SCI) Computer Use and File Sharing

Electronic Information
Resource Usage Policy
Introduction

1.1 Use of University electronic information resources is a privilege, not a right. This policy sets out the responsibilities of students who use the electronic information resources at UMHS & IUON.

These include the academic and administrative networks, computer systems and labs, online information resources (Weather hosted on or off campus). Telecommunications systems and all Internet resources accessed through UMHS & IUON systems-

1.2 The electronic information systems at UMHS & IUON are provided for the purpose of instruction, research, personal development and administration. This policy informs students of the University's expectations and their responsibilities. This policy applies to all users of UMHS & IUON system resources, including those who access these resources from off campus.

Scope

2.1 This policy applies to all UMHS & IUON students, staff, and faculty and to all others granted use of

University's information technology (IT) resources whether individually controlled or shared, stand-alone or networked. It applies to all computer and communication facilities owned, leased, operated, or contracted for by UMHS & IUON. Information technology resources include but are not limited to the University's dedicated internet connection, private networks, telephone, fax voice mail, instant messaging, electronic collaboration, content management, or other applications that attach, utilize, or otherwise interface with UMHS & IUON's data and voice network computing infrastructure. Electronic communications include but are not limited to any information- data, text, graphics, audio, video, or other artifact – that can be sent or received via an electronic system or manipulated or transferred via the network computing infrastructure or an attached device or peripheral.

Policies
Privacy, Integrity and Operational
Security

3.1 The privacy of all users and the integrity and operational security of UMHS & IUON's information technology system must be respected by all. The University's resources must not be used by anyone to gain or attempt to gain unauthorized access to private information, even if that information is not securely protected or is otherwise available. The fact that an individual account and its data may be unprotected does not confer either an ethical or legal right to access it.

Investigations of misuse, unauthorized use, or illegal activity, compliance with federal, state or local laws or regulations, as well as routine or emergency maintenance of the IT system, may require observation of electronic information by appropriate and authorized university officials, employees, or their authorized agents. Such activities are not in violation of this principle so long as these activities are conducted by authorized individuals on behalf of UMHS & IUON and are governed by professional

IT forensic protocols.

3.2 Unauthorized access to private information constitutes a violation of this policy, and may result in disciplinary actions under the Faculty Manual, Student Handbook, HR policies, or other applicable policy statements. Violation of this principle may also constitute a violation of state or federal law.

Use

Use of UMHS & IUON's network computing and electronic communications infrastructure comes with certain responsibilities and obligations.

4.1 Unlawful Use

.
In posting information via e-mail, IM or various social network communications you may not present yourself as an official representative or spokesperson for the University.

.
You may not represent yourself as another person.

- Display of vulgar language.

- Display of language or photographs that imply disrespect for any individual or group because of age, race, gender, ethnicity, or sexual orientation.

- You may not report private (protected) academic information of another student. Such information might include, but is not limited to: course grades, evaluations and examination scores.

- Copying, pirating, or downloading software and electronic files without permission.

- Sending or posting confidential material, trade secrets, or proprietary information outside of the organization.

- Violating copyright law.

- Failing to observe licensing agreements.

- Jeopardizing the security of the organization's electronic communications systems.

- Copying, pirating, or downloading software and electronic files without permission.

- Sending or posting messages that defame or slander other individuals.

- Wasting the University's resources for one's personal gain.

- Stealing or using another individual's account username or password.

- Presentations of photographs that may reasonably be interpreted as condoning irresponsible use of alcohol, substance abuse, or sexual promiscuity. When using these social networking sites, students are strongly encouraged to present themselves in a mature, responsible, and professional manner. Discourse should always be civil and respectful. Moreover, once an item is posted on a network site, it may not be easily removed. Future University administration, program directors, residency directors & employers may review these network sites when considering potential candidates for employment. You certainly want these individuals to have a positive opinion of you.

Intellectual
Property

5.1 At the heart of any academic or research endeavor resides the concept of intellectual property. All copyrighted information (text, images, icons, programs, video, audio, etc.) retrieved from computer or network resources must be used in compliance with applicable copyright and other law. Copied material must be properly attributed. Plagiarism of digital information is subject to the same sanctions

As apply to plagiarism in any other media. Acquiring or sharing copyrighted materials without obtaining the appropriate licenses or permissions may be unlawful.

Unauthorized reproduction of copyright material is prohibited and constitutes Infringement that carries the risk of civil and criminal liability to both the University and the student, as set out in Title 17 United States Code. Chapter 5: <http://www.copyright.gov/title17/92chap5.html>

5.2 Plagiarism is prohibited and is a violation of the Student

Honor and Conduct Codes.

Violation of this policy is subject to University administration disciplinary action, to dismissal.

Violation of Student Honor and Conduct Codes

6.1 UMHS & IUON maintains high standards for its students and various codes and policies govern and inform a student's day to day life in the conduct of his or her University experience. Students are prohibited from using the network computing assets for activities that violate the conduct code, the honor code, or other policies and regulations delineated by The Student Handbook.

Fiduciary Responsibilities

7.1 Faculty Members

Faculty members

possess a great personal responsibility to themselves and to other community members to utilize technology while maintaining their fiduciary responsibilities. These responsibilities include, but are not limited to: Being responsible for the security of one's personal information

Protecting

personal and private information of others. Taking care to minimize risks of various undesirable events, such as disclosure of sensitive personal information, identify theft, and even threats to personal

Safety when using UMHS & IUON information technology assets.

Information Technology Professionals

8.1 IT personnel

University IT personnel is granted elevated or privileged access to UMHS & IUON University's information and information systems. This privileged access places the IT professional in a higher level of trust. To maintain this level of trust, University IT professionals must develop, maintain, and continually enhance their skills and abilities on behalf of those they serve. IT professionals employed by the University must strive to be

trusted and highly skilled custodians through:

- Preserving confidentiality

- Protecting data and information
integrity

- Establishing and maintaining availability
of information systems

- Educating those around them about IT
and social risks related to information systems

- Enhancing and maintaining technical
skills

Due Process; Complaints and Sanctions

9.1 Violations of the policy stated here are treated like any other UMHS & IUON policy violation and are governed by the same procedures. Notification of possible violations may be made to the campus Information Technology Department (IT) Help desk, at Ext 144 & 145 or to abuse@umhs-sk.net

9.2 In particular, the person against whom the complaint is made will be presumed innocent until proven otherwise. Nonetheless, through status should not be altered pending

action on charges, system administrators are authorized to immediately take actions such as locking accounts when the safety and well-being of students; faculty, staff or property is at risk. As soon as practical, the ITS Director will be contacted to either authorize or suspend an investigation. The means of investigating may include, but not be limited to, monitoring traffic and files, including the contents thereof. The subject will be notified of the investigation, and of his or her rights, including the right to due process, as soon as practical.

Evolving Policy

10.1 The University's ITS policies are designed to reflect current conditions. As information technology continues to develop and conditions change, we will review our policies accordingly.