SJMHS Human Resources Policy

Associate Use of SJMHS/Trinity Health-Owned Communications Equipment and Services

Section Number 600 - Work Rules and Corrective Action Policies
Policy Number 632

Effective Date: 12/01/01
Revised Date: 05/01/04; 07/01/08; 1/12/12

Approved by: Rob Casalou, President and CEO

Policy:

The purpose of this policy is to require that all users of Saint Joseph Mercy Health System Health (SJMHS/Trinity Health) owned electronic communication equipment and services use the equipment and services in an appropriate manner.

Users of information accessed via SJMHS/Trinity Health owned electronic communication equipment and services have the responsibility to protect that information in a responsible manner consistent with the best interests of SJMHS/Trinity Health.

SJMHS/Trinity Health reserves the right to access, examine and otherwise monitor use of its communications systems and data files at any time, with or without prior notice, to insure that communications systems are being used only for business reasons and approved personal reasons and in strict compliance with applicable laws including copyright, other SJMHS/Trinity Health requirements, policies and procedures. This includes monitoring of e-mail, voice-mail, real-time monitoring of telephone conversations, and any other transmission via SJMHS/Trinity Health-owned communications equipment and services.

SJMHS/Trinity Health-owned electronic communications equipment and services includes, but is not limited to, networks, systems and related information technology and equipment, wireless connectivity, internal mail systems, telephones, pagers**,** facsimile transmission, computers, computer devices, printers, and scanners and all information conveyed, printed, contained in data files, posted or transmitted either electronically through voicemail, pagers, e-mail and Intra/Internet are the property of the SJMHS/Trinity Health.

SJMHS/Trinity Health associates are prohibited from providing any unauthorized access to SJMHS/Trinity Health-owned communications equipment and services.

TIS must be consulted to evaluate and approve the purchase of any personal computers, PC software, operating systems, services, or peripheral equipment of any kind that are intended for installation on the SJMHS/Trinity Health network.

No one outside TIS is authorized to install, printers, servers, information technology and equipment or provide access to services on the SJMHS/Trinity Health network.

No software may be downloaded or installed onto the PC's or servers on the SJMHS/Trinity Health network from personal devices or the Internet without prior approval of TIS. This includes all software, software updates, and all software plug-ins.

Networked devices may not be connected to a modem without the prior approval of Trinity Information Services.

It is acceptable to use SJMHS/Trinity Health-owned electronic communications equipment and services to fulfill job functions as approved by SJMHS/Trinity Health. Approved use of communications and computer equipment, wireless connectivity, email, Intra/Internet, and network services includes activities related to providing patient care, communicating for the purpose of conducting business, reviewing web sites for product information and services, and researching medical, regulatory or technical information that is appropriate to fulfill job functions. Use of social media is restricted to personally assigned computing devices and must not be accessed via Computers On Wheels (COWS) or computers in alcoves or other patient care areas. Computer devices established for patient/family use

are restricted to patients/families only.

Use of the "All-e-mail" distributions lists, i.e., All SJMHS, All SJMH, All SJMLH, SJMSH, etc. are limited to the following individuals:

Assistant to SJMHS President and CEO
Director, Information Services
Desktop and Network Services Manager, Trinity Information Services
Organizational Leader Administrative Services
Organizational Leader, SJMLH
Organizational Leader, SJMSH
VP, Marketing
VP, Human Resources
Manager, Internal Communications

E-mail users who have reason to send e-mails to All SJMHS, All SJMH, All SJMLH or All SJMSH are required to send their e-mail draft to the appropriate individual listed above for review and approval. Approved e-mails will then be sent to the desired "All" distribution.

Users of SJMHS/Trinity Health communications systems (includes both senders and recipients) are required to comply with HIPAA Privacy regulations as well as SJMHS/Trinity Health and State and Federal statutory confidentiality requirements and all other SJMHS/Trinity Health policies.

E-mail and voice-mail transmissions should not be considered private and may be read or intercepted by others through inadvertent disclosure and accidental or purposeful transmission or retransmission to outside parties or internal parties with possible adverse results and/or damages for the user and/or SJMHS/Trinity Health. Patient identifiable information must not be communicated or transferred using E-mail, the World Wide Web or other Internet communications unless that communication is encrypted with an approved encryption process..

Users of SJMHS/Trinity Health communications system do not have a personal privacy right in any matter created, received or sent via SJMHS/Trinity Health owned electronic communications equipment including voice-mail or e-mail.

SJMHS/Trinity Health reserves the right to access, examine and otherwise monitor use of its communications systems and data files at any time, with or without prior notice, to insure that communications systems are being used only for business reasons and approved personal reasons and in strict compliance with applicable laws including copyright, other SJMHS/Trinity Health requirements, policies and procedures. This includes monitoring of e-mail, voice-mail, real-time monitoring of telephone conversations, and any other transmission via SJMHS/Trinity Health-owned communications equipment and services.

Use of SJMHS/Trinity Health communications systems constitutes agreement by the user to:

a. comply with State, Federal, and HIPAA regulations as well as this policy and all other related SJMHS/Trinity Health policies and procedures, and
b. acknowledge SJMHS/Trinity Health's right to monitor use of the communications systems. Users are required to disclose their personal passwords to SJMHS/Trinity Health/management representatives only.

Guidelines

1. General Network User requirements other than those stated above:

a) Users maintain responsibility for all activities having occurred through the use of either user ID or password;
b) Log out of all computer systems when leaving a workstation unattended for an extended period of time or, if for a shorter period of time, utilize a SJMHS/Trinity Health-approved screen saver with the password function activated and set for period of computer inactivity of ten (10) minutes or less if necessary;
c) Be responsible for the security of accounts and password;
d) Report security violations immediately to Trinity Information Systems and SJMHS Human Resources;
e) Comply with all third party software licenses (any software that is not licensed shall be immediately removed from the computer);

f) Contact Trinity Information Systems for assistance if there are any questions on, or uncertainty of any of the above requirements, or are otherwise unable to comply with any of the above.
g) PCs accessing any network resource must have active, up-to-date virus protection software running on them.

2. Prohibited Use

The following list includes but is not limited to examples of prohibited uses of SJMHS/Trinity Health information systems Network:

a) Misrepresentation of oneself, or inappropriately representing Trinity Health or Saint Joseph Mercy Health System in Internet utilization and communications, including social media.
b) Communications which are demeaning, defaming, harassing including sexually, or discriminatory against any person.
c) Carelessly utilizing any system component, which negatively impacts network performance or unduly jeopardizes network or computing capabilities. This includes, but is not limited to Internet use, Wireless connectivity connectivity, printing, data storage, email, voice mail, or telephone usage.
d) Unauthorized solicitations and uploading of information to the Intranet which is not specifically approved by SJMHS/Trinity Health policy, administration, or department management.
e) Any violation of established copyright or other public laws; and, any activity that may be deemed malicious in nature.
f) Accessing confidential or privileged information that is not required within the scope of one's work.
g) Dissemination of proprietary, strategic, confidential, private or otherwise restricted information without appropriate approvals and proper security controls.
h) Any action that damages or disrupts computing systems or networks, alters their normal performance, or causes them to malfunction regardless of location or duration.
i) Willfully or negligently introducing a computer virus, Trojan horse or other destructive program into the SJMHS/Trinity Health Network, systems or into external systems or networks.
j) Unauthorized decrypting or attempted decrypting of any system or user passwords or any other user's encrypted files.
k) Any use of misrepresentation/fraud to gain unauthorized access to a computing system or network.
l) Attempt to establish a separate Internet linkage or Internet service (including e-mail) or utilization of the network provided Internet utilities for unauthorized or unsupported purposes.
m) Access, display, storage, or distribution of offensive, discriminatory, or pornographic material; or is otherwise inconsistent with or in violation of the mission or policies of SJMHS/Trinity Health; or that contributes to an intimidating or hostile work environment.
n) Participating in contests, games, on-line gambling or accepting promotional gifts for personal use.
o) Using the e-mail account of another individual
p) Forwarding e-mail generated within the SJMHS/Trinity Health to an address outside the SJMHS/Trinity Health/Trinity Health Network without the consent of the author or originator, unless the content of such e-mail is clearly public in nature.
q) Using the SJMHS/Trinity Health e-mail system for non-SJMHS/Trinity Health commercial endeavors or to send chain letters.
r) Broadcasting unsolicited personal views on social, political, religious or other non-business related matters.
s) The use of FTP, unless approved by TIS, is prohibited.
t) While non-Trinity WEB based email access is allowed, non-Trinity email servers are not allowed to run from the SJMHS/Trinity Health network.
u) Remote control applicationsare prohibited.
v) Reconfiguring or tampering with virus protection, firewall, or any other TIS configured software is prohibited.