SUBJECT:	Company Computer Systems
POLICY NO:	VIII:08
APPLICABLE TO:	All Employees
PAGE NO:	1 of 3
EFFECTIVE DATE:	November 1, 2000
REVISION DATE:	August 1, 2018 (due to name change)

I. POLICY:

The Hennepin Healthcare Research Institute (HHRI) provides many of its employees with computers to be used for business related activity. Computer resources are assets of HHRI and are to be protected from unauthorized access, modification, destruction or disclosure. HHRI reserves the right to monitor computer systems and to read and copy all files or data contained on any computer (including but not limited to e-mail messages) at any time and with or without prior notice.

Individual passwords for computers are confidential and should not be shared or posted. If a user's password is learned by someone else, it should be changed immediately. Each user will be responsible for activity performed using the user's password. No user should attempt to obtain access to another user's documents without prior authorization. An active computer, terminal or printer should not be left unattended for any extended period unless protected from unauthorized viewing or used by a password-protected lock such as a screensaver. When working on computers in the work place, users should always use discretion regarding confidential information or non-work related information.

Failure to follow this policy may result in disciplinary action up to and including termination.

II. E-MAIL

The principal purpose of electronic mail (e-mail) is business communications. All e-mail sent through HHRI (from or to) is the property of HHRI (whether or not related to personal matters). E-mail should be treated like all other verbal or written business communications. Appropriate language and standards of decency must be used. Offensive, demeaning, defamatory, harassing or disruptive messages are prohibited.

E-mail that contains confidential or proprietary information must be treated as confidential. No one shall provide e-mail access to an unauthorized person or access another user's e-mail without authorization.

III. INTERNET ACCESS

Any connection between the HHRI corporate network and the Internet presents an opportunity for non-HHRI employees to access corporate systems and information. It is therefore the policy of HHRI to ensure such a connection is secure, controlled, and monitored. Employees authorized to have Internet access should use the Internet for increased productivity rather than for non-business purposes that may adversely affect the security or responsiveness of critical business systems on the network.

Access to Internet E-mail requires managers' approval. Those employees whose jobs require access to the World Wide Web will be permitted to have access only with the approval of their division head/director.

Anti-virus software is installed on all HHRI computers. Users are responsible for using the software to explicitly check file attachments and downloaded files.

Only authorized MIS personnel may establish Internet or other external network connections. Other connections may cause unauthorized access to HHRI's systems and information and are prohibited.

HHRI maintains a log of all Internet-related activities, including e-mail messages and connections to web sites. Although HHRI does not actively monitor these logs, they may be viewed during the course of regular maintenance or when investigating improper conduct.

Examples of permitted uses:

1. Sending and receiving business-related e-mail.
2. Sending and receiving short personal e-mail.
3. Subscription to an Internet mailing list if the subscription is work related and does not generate numerous messages.
4. Downloading files from business-related sites must be scanned for viruses.
5. Reading pre-approved newsgroups for business purposes.

Examples of prohibited (terminable) uses:

1. Sending or arranging to receive file attachments in personal e-mail.
2. Posting, viewing, downloading or otherwise receiving or transmitting offensive, defamatory, pornographic or sexually explicit material.
3. Engaging in computer "hacking" or other related activities.
4. Conducting personal business such as buying and selling personal items.
5. Downloading files for non-business related purposes.
6. Sending sensitive information through Internet e-mail (e.g. Patient information).
7. Posting submissions to newsgroups.

IV. NON-BUSINESS PURPOSES

HHRI computers should primarily be used for HHRI business. However, during an employees scheduled break time, they may use their computer for personal use, provided it does not adversely affect the responsiveness of critical business systems on the network, and is consistent with HHRI's policies and procedures. Users conducting non-business on computers should use discretion.

V. ADDING SOFTWARE

Most proprietary software licenses have legal restrictions prohibiting unauthorized use and copying. Each user is responsible for compliance with these legal restrictions. All software used on any HHRI computer, (including software available on the Internet) must be approved in advance by MIS. Only personnel authorized by MIS may load software onto any HHRI computer, connect any hardware or other equipment to any HHRI computer, or move or change any HHRI computer equipment.

VI. RESPONSIBILITY

A. Each user will be responsible for activity performed using their password.
B. Employees requesting Internet access will be required to sign an acknowledgement that they agree to abide by the terms of this policy, and that failure to do so may result in disciplinary action, up to and including termination.

C. MIS must have appropriate approvals prior to setting up any user with access to Internet E-mail and/or Internet Browsing.

D. The user should contact MIS before downloading any file if the user has questions about a potential virus or reason to believe that the file poses particular risks.