NYGH

POLICY & PROCEDURE

NUMBER: X-15

SUBJECT: **Email**

CROSS REFERENCE:

DATE ISSUED: November, 2001
DATE REVIEWED: February, 2008
DATE REVISED: February, 2008

AUTHORIZATION:

1. INTRODUCTION

North York General Hospital has an Internet-based mail system that provides the ability to send email messages to other hospital employees as well as to any user in the global community who has a valid Internet email address. This includes the ability to send file attachments including word processor documents, spreadsheets, presentations and databases. While email is an extremely useful tool and is used extensively throughout the organization, it is important that all users understand its limitations and particularly the issues associated with personal privacy and organizational security.

2. PURPOSE OF EMAIL AND OWNERSHIP

North York General Hospital encourages the business use of electronic communications, specifically email and Internet. North York General Hospital electronic communications systems generally must be used only for business activities. Incidental personal use is permissible so long as it does not:

(a) consume more than a trivial amount of resources
(b) interfere with worker productivity
(c) compromise patient or staff privacy and confidentiality, and
(d) compromise confidential information that is held in trust with hospital vendors or other agents.

All messages generated on or received by the hospital email system are considered to be the property of North York General Hospital. This includes all messages generated or received by hospital staff and affiliates including volunteers, physicians, students and contract workers. More specifically, any messages originating from or sent to an email address containing the internet domain name nygh.on.ca are considered hospital property with the exception of messages generated by third parties who

have clearly noted copyrights on their messages or the attachments which these messages might contain.

3. PERSONAL PRIVACY

Except as otherwise specifically provided, employees may not intercept or disclose, or assist in intercepting or disclosing, electronic communications. North York General Hospital is committed to respecting the rights of its employees, including their reasonable expectation of privacy. It is the policy of North York General Hospital not to monitor the content of electronic communications, except in **special** circumstances.

If a staff member leaves the employ of the hospital, any messages remaining in that staff member's email inbox or other email folders are considered the property of North York General Hospital and may be viewed, transferred or deleted by the staff member's manager or manager's designate. This will be facilitated by Information Services.

Special circumstances which might result in viewing or monitoring the content of electronic messages include but are not limited to suspicion of tampering with the email system, criminal investigation or the breach or compromise of patient or staff privacy or hospital confidential information. In these or similar circumstances, the immediate supervisor of the department/unit where the staff member works may obtain the assistance of Information Services to view the contents of the staff members email messages.

4. USER ACCOUNTABILITY

Identity

Misrepresenting, obscuring, suppressing, or replacing a user's identity on an electronic communications system is forbidden. The user name, electronic mail address, organizational affiliation, and related information

included with electronic messages or postings must reflect the actual originator of the messages or postings.

Password
Employees will have a private password that controls access to their private mail account. Regardless of the circumstances, individual email passwords must never be shared or revealed to anyone else besides the authorized user. If users need to share computer resident data, they should utilize message forwarding facilities, public directories on local area network servers, and other authorized information-sharing mechanisms.

Reporting Security Alerts
Users must promptly report all information security alerts, warnings, suspected vulnerabilities, and the like to the Information Systems Help Desk (6074). Users are prohibited from utilizing North York General Hospital systems to forward such information to other users, whether the other users are internal or external to the hospital.

Public Representation
No media advertisement or electronic bulletin board type posting or any other public representation about North York General Hospital may be included in an email message unless it has first been approved by the Public Relations Department.

Junk Email
When workers receive unwanted and unsolicited email (also known as spam), they must refrain from responding directly to the sender. Instead, they should forward the message to the IS Director at North York General Hospital who can then take steps to prevent further transmissions. To respond to the sender would indicate that the user-ID is monitored regularly, and this would then invite further junk email.

5. MESSAGE CONTENT

Harassing or Offensive Materials

North York General Hospital computer and communications systems are not intended to be used for, and must not be used for the exercise of the workers' right to free speech. The general policy on harassment in the workplace (III-c-30) applies to the content of email messages.

Message Copying (CCing)

Carbon Copy lists should include only those individuals who are directly involved with the item being communicated or who are thought to require the information contained within for current or future information purposes. Employees must not employ the email system or other internal information systems in such a way that the productivity of other workers is eroded; examples include chain letters and broadcast charitable solicitations.

Attachments

To prevent virus proliferation, attachments can only be opened if the sender *and* the name of the attachment are known. It is the recipient's responsibility to ensure that the attachment is legitimate by contacting the sender. If it is suspected that a mail account has been infected with a virus, that account will be temporarily disabled by Information Services in order to limit the effects of the virus in the organization. IS will contact the user and/or the user's manager when a mail account is disabled.

6. MESSAGE CONFIDENTIALITY

Employees are reminded that North York General Hospital electronic communications systems are not encrypted by default. If sensitive information must be sent by electronic communication systems, encryption or similar technologies to protect the data must be employed.

North York General Hospital cannot guarantee that electronic communications will be private. Employees should be aware that electronic communications can, depending on the technology, be forwarded, intercepted, printed, and stored by others.

Clinical information, patient information or administratively sensitive information may be communicated via email internally, but must not be sent to recipient(s) outside the hospital unless secure (encrypted) mechanisms have been installed.

Message Forwarding

Recognizing that some information is intended for specific individuals and may not be appropriate for general distribution, electronic communications users should exercise caution when forwarding messages. Sensitive information must not be forwarded to any party outside North York General Hospital without the prior approval of a department manager.

With the exception of emergencies and regular system maintenance notices, broadcast facilities must be used only after the permission of a senior manager has been obtained. Broadcast facilities will be provided only to designated staff including senior management (or designate), the Director of Corporate Communications, and the Director of Information Services.

7. ADMINISTRATION OF THE EMAIL SYSTEM

System Protection

If it is suspected that a mail account has been infected with a virus, that account will be temporarily disabled by Information Services in order to limit the affects of the virus in the organization. IS will contact the user and/or the user's manager when an email account is disabled.

User Back-Up

If an electronic mail message contains information relevant to a clinical event, or an administratively sensitive item, it should be retained for future reference. Most electronic mail messages will not fall into these categories, and accordingly can be erased after receipt. Users must regularly move important information from electronic mail message files to word processing documents, databases, and other files. The email system is not intended for the archival storage of important information.

Statistical Data

Consistent with generally accepted business practice, North York General Hospital collects statistical data about electronic communications. As an example, statistics of the number of undeliverable messages per month and directory sizes are routinely compiled. This data allows Information Services to ensure the ongoing availability and reliability of the system.

Purging Electronic Messages

Users must periodically purge messages that are no longer needed from their personal electronic message storage areas. Each user will be allocated a specific storage area and size on the mail server. Users that exceed their message storing capacity on the server will be duly notified by IS.