ST. JOSEPH HOSPITAL

Original: *10/1996*
Review: *01/2016*
Next Review: *01/2019*
Policy Champion: *Wesley Layne: Director of Human Resources*
Policy Area: *HR - Employment*
Applicability: *Nashua St. Joseph Hospital*

Telephone and Computer Resources, MG-16

PURPOSE:

The purpose of this policy to ensure that St. Joseph Healthcare telephones, computers, e-mail and the Internet are available for matters which affect our patients' safety and welfare, emergencies, and routine company business and to assure that employees use personal cell phones and devices in accordance with this policy.

SCOPE:

St. Joseph Healthcare

POLICY:

Telephone Usage

Telephones are to be used for calls affecting our patients' safety and welfare, emergencies, and routine company business. Personal calls during the work hours can interfere with employee productivity, safety, and can be distracting to others.

St Joseph telephones are for business purposes only. While there may be rare occasions when employees need to use the telephones for personal use, it is expected that such usage will be within reasonable, brief limits, and that employees will charge all long distance personal calls to their personal telephone credit card, home telephone number, or call collect. Employees needing to make personal telephone calls may also use their personal cell phones. In general personal calls should be limited to breaks and the lunch period except in case of emergency.

If you need to give out your work number in order to receive personal calls please provide the person(s) with your direct dial line. If your work station does not have a direct dial line, please provide the person(s) with: the hospital express line number(595-5300); the extension of your workstation; and the name of your department/ unit.

Personal Cell Phone Usage

while at work employees are expected to exercise the same discretion in using personal cell phones as is expected for use of the company's phones. Personal cell phone use and text messaging should be limited to breaks and meal periods.

While at work, personal cell phones should be turned off except in the event of an employee is awaiting an important call in which case the cell phone should be set on vibrate mode.

Employees are also prohibited from using their personal cell phone cameras to photograph any company documents or property or any other person, not limited to co-worker; patient; visitor, at the workplace without his or her knowledge or permission.

St. Joseph Healthcare will not be liable for the loss of personal cell phones brought into the workplace.

Work-related cell phone calls, texting or e-mailing while driving is prohibited.

Voicemail Usage

The voicemail system is the property of St. Joseph Healthcare and is intended for legitimate business use only. The company reserves the right to monitor the system to enforce policies regarding business use, harassment, and to access information without prior notice. Employees should have no expectation of any personal privacy rights in any voicemail messages created, received, or sent through the voicemail system.

Directors will have the responsibility of establishing in their area(s) protocols for checking individual voicemail boxes in the absence of an employee(s). Typically, an authorized individual in the area(s) will have the responsibility to check voicemail boxes) of an absent employee. This is to ensure that company business, and thus appropriate customer service, can be maintained during any employee(s) absence.

Voicemail may also be programmed to **not** receive messages during an individual's absence.

Please also see Attachment A for guidance.

Computer E-Mail and Internet Usage

Please see Attachment A for guidance.

PROCEDURE:

Telephone Usage

Planning Your Calls:

The telephone expense of St. Joseph Healthcare is substantial. In order to assist the Hospital in controlling this cost it is strongly encouraged that you plan your calls. Before you phone, make an outline of what points you wish to cover. Identify yourself and state the purpose of your call.

Please also see Attachment A for guidance.

Voicemail Usage

- **Courtesy:**

  While our voicemail System is designed to increase productivity, it is expected that you will treat co-workers with respect when leaving messages. Please do not leave curt, last minute messages for anyone. Also, do not use voicemail to "hide" from co-workers or customers. If you are at your desk, it is expected that you will answer your telephone personally.

- **Personal Messages:**

  The voicemail System is not to be used for personal messages such as soliciting contributions for your favorite charity, arranging for an after work get-together or the like. Our system only has a limited amount of disk space for recording messages and, for that reason, it is requested that you limit your messages to business matters only.

- **Greetings:**

  Your greetings should normally be in the following format: "Hello. This is ----------. I am not currently available to take your call. Please leave your message at the tone." Please check with your supervisor to see if there is a preferred format for your department/unit.

If you are away for an extended period of time, you may alter your message to indicate the length of time you will be away from the office. It is suggested that employees set their voicemail to NOT accept messages while they are away for an extended period.

- **Deletions**:

  Due to the limited disk space for message storage, it is required that Phonemail box(es) be checked more than once a day and messages be responded to and then deleted.

Please also see Attachment A for guidance.

Application of Management & Governance Policies

Many Management & Governance Policies apply to the use of both the telephone and voicemail systems. For example, our policies concerning solicitation, harassment, reporting absences and the like, all apply. Using the telephone or voicemail systems to harass or solicit others is expressly prohibited. Employees will be held responsible for any voicemail messages sent through their extension.

One of the features of our telephone service is a Call Accounting System. The **Call Accounting System** provides reports of call activity. These reports will be used to assist the company in analyzing and controlling the cost of telephone usage. The report lists, by individual extension: **outgoing** telephone number(s) dialed; location call was placed to; call duration; and charges; as well as **incoming** telephone number(s) of calls received; call location; and call duration. Call Accounting reports will be reviewed by the Director, Hospitality Services and the Manager, Communications. If concerns arise based on any report, the Director, Hospitality Services or the Manager,

Communications will contact the appropriate supervisor.

Additionally, Directors may request call accounting reports for extension(s) in use in their area(s) from the Manager, Communications. Any abuse of the telephone system will be subject to progressive discipline, per Policy "Rules of Conduct and Discipline, HR-26".

Employees who fail to comply with this policy or other Hospital policies are subject to discipline, up to and including discharge, in accordance with Policy "Rules of Conduct and Discipline, HR-26".

Computer, E-Mail and Internet Usage

Please see Attachment A for guidance here.

Attachment:

Attachment A - Acceptable use of Telephone and Computer Resources

RESPONSIBILITY:

Director, Hospitality Services
Manager, Communications

Director of Human Resources
All employees of St. Joseph Healthcare

Attachments:

Attachment A - Acceptable use of Telephone and Computer Resources

Approval Signatures

Committee	Approver	Date
Senior Leadership Team (on behalf of)	Shirley Lussier: Director of Human Resources	01/2016
	Shirley Lussier: Director of Human Resources	01/2016

Attachment A

Acceptable use of Telephone and Computer Resources

St. Joseph Healthcare (here to after referred to as “St. Joseph”) provides computers, e-mail, voicemail, facsimile communications equipment, and internet access as essential tools to support St. Joseph business objectives. It is the responsibility of each employee to ensure that this technology is used solely for proper business purposes and in a manner that does not compromise the confidentiality of St. Joseph’s proprietary or other sensitive information. This policy applies to each and every employee of St. Joseph Healthcare.

1. All e-mail and voicemail correspondence in St. Joseph communications systems is the property of St. Joseph, regardless of where it may have originated.

2. Employees should not have any expectation of privacy in their usage or anything they create, store, send or receive on the company’s computer resources, including e-mail and voicemail. These communications are not considered private despite any such designation either by the sender or the recipient.

3. Employees should be aware that messages sent to recipients outside of St. Joseph, if sent over the Internet and encrypted, are not secure. Accordingly, no St. Joseph or client confidential information should be sent over the Internet except by St. Joseph approved means. If in doubt, ask the Director, Risk Management/ Privacy Officer.

4. St. Joseph reserves the right but does not have a duty to monitor and examine without prior notice the contents of St. Joseph communications system, including e-mail, voicemail, facsimiles, internet sites visited chat rooms and newsgroups, material downloaded or uploaded by employees to the Internet or other computer resources, at St. Josephs discretion and for any purpose. St. Joseph reserves the right to disclose the contents of any such material for any purpose and to any person St. Joseph deems appropriate or desirable. If you wish to communicate privately, do not use St. Joseph’s communication system.

5. The existence of passwords and “message delete” functions do not restrict or eliminate St. Joseph’s ability or right to access electronic communications. Even the deleted messages may be recovered and reviewed.

6. Employees shall not share passwords, or provide e-mail/voicemail access to an unauthorized user, or access another user’s e-mail/voicemail box without authorization.

7. Employees who use their own equipment to connect to St. Joseph from outside St. Joseph premises or from home should know that any communications that are delivered to or sent through St. Joseph communications system, are not private, and are subject to all of the terms and provisions of this policy statement.

8. Employees shall not post, display or make easily available any access information, including, but not limited to, passwords.

9. St. Joseph's communication and computer systems are intended for business use. However, it is recognized that there may be rare occasions when employees need to use the communication and computer system for personal use. Personal use is permitted on a limited, reasonable basis **and should be limited to breaks and meal periods.** However, **solicitation** for any outside business, commercial or organizational purpose is **prohibited at all times.**

10. Harassing, defamatory, threatening or discriminatory messages are prohibited. This includes, but is not limited to, messages that are inconsistent with St. Joseph's policies concerning equal employment opportunity and sexual and other unlawful harassment and discrimination.

11. Messages sent to "All Employees" and other broadcast messages should be used sparingly, and only for St. Joseph and client business. These messages must be approved by the appropriate VP and sent through "System Manager".

12. St. Joseph's network, including its connection to the Internet, is to be used primarily for business and client related matters. Unauthorized use of the Internet is strictly prohibited. Unauthorized use includes, but is not limited to:

    - Unauthorized entry or attempted unauthorized entry into other computer systems or areas of the St. Joseph computer systems which you are not authorized to view;
    - Attempting to disable or compromise the security of information contained on St. Joseph's computers;
    - Intentionally introducing a virus or other mischievous software onto any St. Joseph computer;
    - Downloading or posting of pornographic or sexually explicit material; and
    - Internet messages should be treated as non-confidential. Anything sent through the Internet passes through a number of different computer systems, all with different levels of security. The confidentiality of messages may be comprised at any point along the way, unless the messages are encrypted.

13. Any Internet Postings are prohibited without proper St. Joseph authority. Under no circumstances shall information of a confidential, or otherwise proprietary nature be placed on the Internet including but not limited to web pages, chat rooms, newsgroups, online services, messaging systems, social networking sites (such as myspace), blogs and bulletin boards, except as specifically authorized by St. Joseph.

14. Employees are prohibited from engaging in online social networking (e.g. facebook, myspace, twitter, etc.) and internet blogging activities while on company time, property or business.

15. Employees are prohibited from using St. Joseph's company e-mail address in their personal profiles on social networking sites.

16. Employees engaging in online social networking and blogging activities may not defame, harass, or threaten St. Joseph, its employees, services, clients, partners, affiliates, vendors and suppliers, and competitors (and their services. An Employees online social networking and blogging activities must contain a disclaimer that the views and opinions they express about work-related matters are their own, have not been reviewed or approved by St. Joseph, and do not necessarily represent the views and opinions of St. Joseph.

17. Subscriptions to news groups and mailing lists are permitted when the subscription is for a work-related purpose. Any other subscriptions are prohibited.

18. Information posted or viewed on the Internet may constitute material subject to copyright. Therefore, reproduction of information posted or otherwise available over the Internet may be done only by express permission from the author or copyright holder.

19. Unless the prior approval of management has been obtained, users may not establish Internet or other external network connections that could allow unauthorized persons to gain access to St. Joseph systems and information. These connections include the establishment of hosts with public modem dial-ins, World Wide Web home pages and File Transfer Protocol (FTP) servers.

20. All files downloaded from the Internet must be checked for possible computer viruses. If uncertain whether your virus-checking software is current, you must check with Information Systems before downloading.

21. St. Joseph has provided wireless Internet (wifi) access in certain areas of the Hospital for patients and visitors. Employees are free to make use of this service under all of the same conditions and restrictions as apply to Internet

access by any other means. Wifi Access is available through a self-pay, daily charge method.

Any employee who violates this policy may be subject to discipline, up to and including discharge in accordance with HR-26.