	The Johns Hopkins Health System	<i>Policy Number</i>	SYS010
	<b>PFS Policies and Procedure Manual</b>	<i>Effective Date</i>	06/01/04
	<i>Subject</i>	<i>Page</i>	1 of 4
	<b>Computer Usage Policy</b>	<i>Revised</i>	4/24/06

## **POLICY**

This policy applies to the Johns Hopkins Health System (JHHS) Patient Financial Services (PFS) Department.

## **PURPOSE**

Users of the JHHS network and computer resources have a responsibility not to abuse the network and resources and to respect the rights of others. This policy provides guidelines for the appropriate and inappropriate use of information technologies.

## **PROCEDURES**

The purpose of electronic systems and communications resources is for work-related activities.

## **REFERENCE**


Johns Hopkins Information Technology User Policies,  
<http://www.it.jhu.edu/policies/itpolicies.html#UseofIT> (Exhibit A)

### **Desktops:**

- Personal Screen Savers are prohibited.
- Personal Wallpaper is prohibited.
- You cannot install any personal software.
- Storing, processing, or transferring of any files not specifically related to an individual's job duties is prohibited.

### **E-Mail:**

- Use of electronic communications (such as GroupWise) to send obscene, threatening, fraudulent, or other messages in violation of laws or JHHS policy is strictly prohibited. JHHS provides e-mail to employees for business purposes. Whenever a user sends an e-mail, their name, user id, and location are recorded. You must therefore, exercise good judgment and common sense when creating and distributing e-mail messages.
- There is no guarantee of privacy with an e-mail message, and JHHS reserves the right to access all aspects of employees' e-mail at any time and for any reason and without notice to the employee.

	The Johns Hopkins Health System	<i>Policy Number</i>	SYS010
	<b>PFS Policies and Procedure Manual</b>	<i>Effective Date</i>	06/01/04
	<i>Subject</i>	<i>Page</i>	2 of 4
	<b>Computer Usage Policy</b>	<i>Revised</i>	4/24/06

- **Internet Usage:**

- Internet usage will be monitored.
- Excessive non-business usage not allowed.
- Users may access the Internet to carry out legitimate business purposes.
- Access is a business privilege conditional upon adherence to policies and procedures.
- Users should treat the Internet as they would any other written communication, anything created on the computer or Internet may, and likely will, be reviewed.
- Sending, receiving, displaying, printing, of material that is fraudulent, harassing, illegal, embarrassing, sexually explicit, obscene, or intimidating, is prohibited. Employees encountering such material should report it to their supervisor or manager immediately.
- Users wishing to download any file or software from non- JHHS sources must contact the IS department or immediate supervisor or manager prior to downloading. Downloading of files or software can endanger the network at large, or the user's individual PC to the threat of computer viruses.

Computer systems are a standard means of business at JHHS. The information contained in them includes patient records, financial, business documents, and Human Resources data. We all get some sort of computerized information whether on-line or printouts and we all need to protect that information.

Practical ideas for computer security:


Keep information confidential

- Do not reveal information or discuss it with anyone who does not **need to know**.
- All information regarding business operations belongs to JHHS.
- All patient information belongs to the patient.

Be conscious of your environment

- If you print something pick it up from the printer promptly.
- Don't leave unattended printouts in an open area.
- Make sure someone is not looking over your shoulder at the monitor.
- When you leave your area remember to save all data and log off to prevent unauthorized access.

Keep your password Confidential

	The Johns Hopkins Health System	<i>Policy Number</i>	SYS010
	<b>PFS Policies and Procedure Manual</b>	<i>Effective Date</i>	06/01/04
	<i>Subject</i>	<i>Page</i>	3 of 4
	<b>Computer Usage Policy</b>	<i>Revised</i>	4/24/06

- Your ID and password identifies you to each system or platform.
- Your password acts as your electronic signature and is comparable to your legal written signature.
- Do not share your password with anyone - you are responsible for actions that another party takes with your password.
- Do not write your passwords down. Keep it in your memory.
- You should have a different password for each system in which you have access; otherwise if someone finds your password to one system, they would have your password to all the systems.
- Change your password every 90 days and if you suspect someone else knows it.

#### Passwords should

- *not* be the same as your user ID or name
- *not* a word in a standard dictionary
- between 6 and 8 characters long and must contain at least one numeric character.

#### Examples of good passwords

- Vanity license plates - UR2COOL
- The first letters of words in a sentence - MWBIJ1 - My Wife=s Birthday Is
- January 1.

#### Report Suspicious Activity


If you suspect someone is misusing the computer system, call JHMCIS Information Security at 5-6831 or the Help Desk after hours at 5-HELP

All computer systems are owned, and operated by the Johns Hopkins Health System (JHHS). All computer systems and related equipment are intended for the communication, processing, and storage of official business or other authorized information only.

All computers are subject to monitoring to ensure proper use of the systems, and to prevent unauthorized use and violations. All employees should be aware that any information placed in the system is subject to monitoring, and is not subject to any expectation of privacy.

If evidence of violation of criminal statutes is revealed, this evidence and other related information may be provided to law enforcement officials.

If monitoring of this or any other system reveals violations of security regulations or unauthorized

	The Johns Hopkins Health System	<i>Policy Number</i>	SYS010
	<b>PFS Policies and Procedure Manual</b>	<i>Effective Date</i>	06/01/04
	<i>Subject</i>	<i>Page</i>	4 of 4
	<b>Computer Usage Policy</b>	<i>Revised</i>	4/24/06

use, this evidence and any other related information may be provided to the appropriate management team.

Employees who violate security regulations or make unauthorized use of the computer systems are subject to appropriate disciplinary action, up to and including termination of employment.

**SPONSOR**

Senior Director, Patient Financial Services, JHHS

**REVIEW CYCLE**

Three (3) years

**APPROVAL**

\_\_\_\_\_  
Senior Director, JHHS

\_\_\_\_\_  
Date

\_\_\_\_\_  
Director, PFS Systems Support, JHHS

\_\_\_\_\_  
Date

## Exhibit A

### IT @ Johns Hopkins

#### **User Policies**

##### **1. USE OF IT RESOURCES**

###### **Acceptable Use**

Acceptable use of IT Resources is use that is consistent with Johns Hopkins' missions of education, research, service, and patient care, and is legal, ethical, and honest. Acceptable use must respect intellectual property, ownership of data, system security mechanisms, and individuals' rights to privacy and freedom from intimidation, harassment, and annoyance. Further, it must show consideration in the consumption and utilization of IT Resources, and it must not jeopardize Johns Hopkins' not-for-profit status. Incidental personal use of IT Resources is permitted if consistent with applicable JH and divisional policy, and if such use is reasonable, not excessive, and does not impair work performance or productivity.

###### **Unacceptable Use**

Unacceptable use of IT Resources includes, but is not limited to:

- a. Unauthorized access to or unauthorized use of JH IT Resources
- b. Use of IT Resources in violation of any applicable law
- c. Harassing others by sending annoying, abusive, profane, threatening, defamatory, offensive, or unnecessarily repetitive messages, or by sending e-mails that appear to come from someone other than the sender
- d. Any activity designed to hinder another person's or institution's use of its own information technology resources
- e. Privacy violations (e.g., disclosure or misuse of private information of others)
- f. Installation of inappropriate software or hardware on IT Resources (e.g., network or password "sniffing" software, offensive applications, and malicious software).
- g. Any use of copyrighted materials in violation of copyright laws or of vendor licensing agreements (e.g. illegal downloading and/or sharing of media files or computer software)
- h. Intentional, non-incident acquisition, storage, and/or display of sexually explicit images, except for acknowledged, legitimate medical, scholarly, educational, or forensic purposes. Exposure and/or display of such material may be offensive, constitute sexual harassment or create a hostile work environment
- i. Security breaches, intentional or otherwise, including improper disclosure of a password and negligent management of a server resulting in its unauthorized use or compromise
- j. Commercial use of IT Resources for business purposes not related to Johns Hopkins
- k. Use, without specific authorization, to imply JH support (as opposed to personal support) for any position or proposition

I. Use to engage in activities, including for example certain political activities, prohibited to tax exempt 501 (c) (3) organizations or that otherwise may result in a hostile work environment.

## **2. E-MAIL USE**

The JH e-mail systems are used to support Johns Hopkins' mission and to allow effective communication between faculty, staff, students, and business associates. These systems vary substantially in size, scope and sophistication. Policies and procedures regarding e-mail storage, back-up, and archiving also vary substantially across JH. In addition, there is no single e-mail archive system for the entire institution. Back-up, storage and archiving of important e-mail messages are the responsibility of each individual user.

E-mail transmission over the Internet is inherently insecure and subject to security breaches that include message interception, message alteration, and spoofing. Users of JH e-mail systems should not assume the confidentiality or integrity of any message that is sent or received via the Internet.

While the transmission and receipt of e-mail messages is generally reliable, timely delivery of time-sensitive information cannot be guaranteed.

### **Acceptable Use**

Acceptable use of e-mail is use that is consistent with the *Use of IT Resources* Policy.

### **Unacceptable Use**

Unacceptable use of Johns Hopkins e-mail systems includes, but is not limited to:

- a. Harassing others by sending annoying, abusive, profane, threatening, defamatory, offensive, or unnecessarily repetitive messages
- b. Sending/receiving individually identifiable health information, social security numbers, passwords, or any other confidential information via the Internet without making reasonable accommodation for the security of such information
- c. Sending e-mail messages from a personal e-mail account that is not owned by the sender without prior approval of the owner
- d. Concealing the identity of the sender, impersonating another, or representing that the sender is someone other than the actual sender
- e. Using JH e-mail to assert or imply that personal views or opinions are the institutional views or opinions of JH
- f. Using JH e-mail systems or address information for any commercial purpose not related to JH
- g. Broadcasting e-mail communications to users or JH e-mail systems without the proper institutional or divisional approval. Such communications are subject to approval by designated JH officials
- h. Intentional distribution of messages that contain viruses, worms, or other malicious code

### **3. ANTI-VIRUS POLICY**

Electronic viruses, worms, and malicious software are constant threats to the security and safety of computer networks and computing environments. These threats can be minimized by using protected equipment and practice of safe computer habits.

All devices vulnerable to electronic viruses must be appropriately safeguarded against infection and retransmission. Johns Hopkins has licensed anti-virus software for use by faculty, staff, and students. It is the responsibility of every user to ensure that anti-virus protection is current. Infected devices may be blocked and/or removed from the JH Network by IT@JH or appropriate departmental personnel.

Effective anti-virus protection includes, but is not limited to:

- a. Installing anti-virus software on all vulnerable devices
- b. Configuring anti-virus software to provide real-time protection
- c. Updating anti-virus software with new virus definition files as soon as available
- d. Utilizing automated anti-virus updates
- e. Executing virus scans on a frequent schedule
- f. Refraining from opening e-mail attachments from unknown, suspicious, or untrustworthy sources
- g. Refraining from downloading files from unknown or suspicious sources
- h. Avoiding direct disk sharing with read/write access unless there is a business requirement to do so
- i. Scanning removable media for viruses before use.