	The Johns Hopkins Health System	<i>Policy Number</i>	SYS031
	PFS Policies and Procedures Manual	<i>Effective Date</i>	6-4-01
	<i>Subject</i>	<i>Page</i>	1 of 10
	Computer Software Policy	<i>Revised</i>	08-12-05

POLICY

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

PURPOSE

The computer systems in the PFS department are intended for the use of conducting business for the Patient Financial Services department, and employees cannot install software without the written consent of the Director, PFS Systems Support. "Computer software" includes, but is not limited to, purchased software, sound, graphics, screen savers, wallpaper, images, shareware, and freeware. No illegally obtained or illegally copied (pirated) software is allowed. Anyone who causes unauthorized software to be installed is in violation of this policy.

PROCEDURES

SOFTWARE STANDARDS

The software that is made available to the user is based on the needs of the individual. The standard software is detailed below.

REFERENCE

Electronic Mail, Computer, and Information Technology Appropriate Use Policy (attached)

- **Operating System:**

Windows 2000

Windows XP

- **JHHS PFS Specific:**

HIP Meditech CS


EPR '98 Meditech Magic

"C" View

- **GroupWare:**

Novell GroupWise

- **Application Suite**

	The Johns Hopkins Health System	<i>Policy Number</i>	SYS031
	PFS Policies and Procedures Manual	<i>Effective Date</i>	6-4-01
	<i>Subject</i>	<i>Page</i>	2 of 10
	Computer Software Policy	<i>Revised</i>	08-12-05

Microsoft Office – Word, Excel, Powerpoint

- **Internet Access**

Internet Explorer

- **Data Base**

Microsoft Access

- **Utilities/Diagnostic**

VPN

PC Anywhere

Norton's Anti-Virus

Adaptec CD-Burner software

Additional Software:

The installation or use of additional software must be approved in writing by the Director, PFS Systems Support. Taking PFS, software home or elsewhere (even for work purposes) must also be authorized by the Director, PFS Systems Support. "Additional software" includes, but is not limited to, screen savers, special graphics programs (such as Adobe), web design software, specific e-mail programs (such as Outlook), special utilities (such as Nero Burn ROM, Snag-It), and other such programs.


Software Training:

Training is provided by the PFS Development & Training Department. The training calendar is provided monthly. Ongoing classes include Introduction to PC's, Word, Internet, Excel, Access, PowerPoint, GroupWise, EPR, Keane, Meditech, RDS and WebX.

Disciplinary Action:

Violation of this policy by employees, will result in disciplinary action according to established JHHS disciplinary procedures.

SPONSOR

	The Johns Hopkins Health System	<i>Policy Number</i>	SYS031
	PFS Policies and Procedures Manual	<i>Effective Date</i>	6-4-01
	<i>Subject</i>	<i>Page</i>	3 of 10
	Computer Software Policy	<i>Revised</i>	08-12-05

Senior Director, Patient Financial Services, JHHS

REVIEW CYCLE

Three (3) years


APPROVAL

Senior Director, JHHS


Date

Director, PFS Systems Support, JHHS

Date

	The Johns Hopkins Health System	<i>Policy Number</i>	SYS031
	PFS Policies and Procedures Manual	<i>Effective Date</i>	6-4-01
	<i>Subject</i>	<i>Page</i>	4 of 10
	Computer Software Policy	<i>Revised</i>	08-12-05

I.	Policy.	2
A.	Statement of Intent, Purpose and Need.	2
B.	Definitions.	2
C.	Scope.	2
D.	Expectation of Privacy.	3
E.	Appropriate Use.	3
	1. Allowable Use.	3
	2. Proper Authorization.	3
F.	Inappropriate Prohibited Use.	3
	1. Use that impedes, interferes with, impairs, or otherwise causes harm to the activities of others.	4
	2. Use that is inconsistent with Hopkins' non-profit status.	4
	3. Disguised use.	4
	4. Misrepresentation.	4
	5. Political, Religious or Similar Use.	4
	6. Harassing or threatening use.	5
	7. Distributing computer viruses.	5
	8. Sexually Explicit Images.	5
	9. Illegal Acts.	5
	10. Copyright Violations.	5
G.	Special Circumstances.	6
	1. Computer Programs.	6
	2. Broadcast Messages.	6
H.	Security and Confidentiality.	6
	1. Confidentiality.	6
	2. Hopkins Intellectual Property and Confidential Information.	6
	3. Encryption.	7
I.	Access to computers or messages.	7
J.	E-mail and Records Retention.	7
	1. Backups.	7
	2. Records Retention.	7
	3. Archives.	8
K.	Policy Violations.	8
	1. Termination of use privileges.	8
	2. Discipline.	8
II.	Reference.	8
III.	Responsibilities.	9
IV.	Sponsor.	9
V.	Review Cycle.	9
VI.	Approval.	9
I.	Policy.	

	The Johns Hopkins Health System	<i>Policy Number</i>	SYS031
	PFS Policies and Procedures Manual	<i>Effective Date</i>	6-4-01
	<i>Subject</i>	<i>Page</i>	5 of 10
	Computer Software Policy	<i>Revised</i>	08-12-05

A. Statement of Intent, Purpose, and Need.

As use of Information technology (IT) systems expands, and resources become increasingly scarce and costly, the need for a uniform policy for IT usage has become evident. Misuse of IT systems, and attacks on and threats to the Hopkins systems have increased with increased usage. The purpose of this Policy is to protect Hopkins systems, advise faculty, students and staff of important use considerations, and to warn faculty, students and staff of inappropriate behavior that could lead to disciplinary action.

B. Definitions.

1. Hopkins means Johns Hopkins University (JHU), the Johns Hopkins Health System (JHHS) all of its schools, divisions, and affiliated corporations, who share IT resources directed by the CIO of JHU and JHHS. Hopkins includes JHPIEGO, and other such entities.

2. IT resources (often referred to simply as resources) includes computers, computer systems, network services, Internet access and E-mail systems including systems assigned to and used by individual employees as well as shared systems.

C. Scope.

Specific policies may be (and have been) adopted which apply to specific use by certain members of the Hopkins population, such as those policies which govern student use. Such policies must be interpreted in conjunction with this policy. However, no specialized policy shall be interpreted to allow what is prohibited under this policy. Classified information shall be handled only in accordance with laws regulating and governing it and is not otherwise specifically addressed in this policy. All use of Hopkins' IT resources is governed by this policy, regardless of the user's location and means of access.


D. Expectation of Privacy.

1. Hopkins IT resources are property of Hopkins. Any data, files, and materials, including E-mail, stored on or transmitted through Hopkins IT resources are and remain Hopkins property and may be accessed by Hopkins as reasonably necessary to protect Hopkins' interests.

2. Although it is not the routine policy of Hopkins IT resource administrators or designees to view others' files, and Hopkins' intention is to keep files private, Hopkins cannot guarantee privacy.

3. Pursuant to the Electronic Communications Privacy Act of 1989, Title 18, United States Code, Sections 2510 and following, notice is hereby given that there are no computer resources provided by Hopkins that guarantee the confidentiality of files on or which pass through those resources. Hopkins reserves and intends to exercise the right to monitor, review, audit, intercept, access, and as necessary or required by law, disclose all messages created, received, or sent over its computer and/or E-mail systems for any purpose.

3. A user of Hopkins' computer resources has no right of privacy in E-mail messages,

	The Johns Hopkins Health System	<i>Policy Number</i>	SYS031
	PFS Policies and Procedures Manual	<i>Effective Date</i>	6-4-01
	<i>Subject</i>	<i>Page</i>	6 of 10
	Computer Software Policy	<i>Revised</i>	08-12-05

downloaded files, or other communications that are created, sent, received, or stored on Hopkins IT resources. Users of Hopkins' IT resources are advised that they should not assume the confidentiality of any message. Further, a personal password does not guarantee the confidentiality of files or messages. Even when a message is deleted or erased, it is still possible to retrieve and read the message.

E. Appropriate Use.

1. Allowable Use. Hopkins' IT resources are provided to promote and benefit the mission of Hopkins. In general, Hopkins IT resources shall be used only to support the research, education, clinical, administrative, and other functions of the institution. Incidental personal use is permitted, so long as such use is kept to a minimum, does not consume regular work hours, does not unduly burden Hopkins IT resources, and is otherwise in conformity with this policy.
2. Proper Authorization. Users are entitled to access only those computer resources that are consistent with their authorization.

F. Inappropriate Prohibited Use.

The following list is not intended to be exhaustive but is exemplary only. Users must conform to the spirit and intent of this policy which will be broadly interpreted.


1. Use that impedes, interferes with, impairs, or otherwise causes harm to the activities of others. Hopkins IT resources shall not be used for purposes that could reasonably be expected to cause, directly or indirectly, excessive strain on any IT facilities, or unwarranted or unsolicited interference with others' use of IT resources. Such uses include, but are not limited to:

Knowingly or recklessly distributing unwanted mail, chain letters or other unwanted messages, (e.g., spamming or improper use of mailing lists);

- Other behavior that may cause excessive network traffic or computing load such as transferring numerous and excessively lengthy files, such as MP-3 files, except as reasonably necessary for Hopkins business.

2. Use that is inconsistent with Hopkins' non-profit status. Hopkins is a non-profit, tax-exempt organization and, as such, is subject to specific federal, state, and local laws regarding sources of income, political activities, use of property, and similar matters. Commercial use of IT resources for non-Hopkins business purposes is generally prohibited, except if specifically authorized and permitted under Hopkins conflict-of-interest, outside employment, and other related policies. Communications and exchanges of data which may have an incidental financial or other benefit to an external organization are permitted, so long as it furthers Hopkins' educational, administrative, research, clinical, and other roles.

3. Disguised use. Users must not conceal their identity when using E-mail or other IT resources. Users are also prohibited from masquerading as or impersonating others or otherwise using a false identity ("spoofing").

	The Johns Hopkins Health System	<i>Policy Number</i>	SYS031
	PFS Policies and Procedures Manual	<i>Effective Date</i>	6-4-01
	<i>Subject</i>	<i>Page</i>	7 of 10
	Computer Software Policy	<i>Revised</i>	08-12-05

4. Misrepresentation. Users shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of Hopkins or any division of the institution unless appropriately authorized (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer shall be included unless it is clear from the context that the author is not representing the institution.

5. Political, Religious or Similar Use. Without specific authorization, IT resources shall not be used to solicit or proselytize for commercial ventures, religious causes or political campaigns, outside organizations or other non-Hopkins related activities.

6. Harassing or threatening use. IT resources may not be used to harass or threaten or to send discourteous or offensive messages. This includes, for example, distribution of offensive material or repeated unwelcome contacts with another person. Words, phrases, statements, threats or other speech that would be considered harassing, threatening, racially or ethnically offensive or would otherwise be improper if stated verbally to the recipient are no less a violation of policy if transmitted by electronic means. For additional information on Hopkins' harassment policies, see (LIST LINKS to HR policy.)

7. Distributing computer viruses. Users shall not knowingly distribute or launch computer viruses, worms, or other rogue programs.


8. Sexually Explicit Images. Except as may be necessary and appropriate for legitimate scholarly purposes, Hopkins prohibits use of its IT resources to access, view, or download sexually explicit images, which Hopkins believes are inappropriate in the workplace, and if tolerated would expose the institution not only to embarrassment, but also the risk of loss of community and donor support. If there is a legitimate scholarly need to access such material using Hopkins' IT resources, disclosure of the need and the type of material to be accessed shall first be made to and the legitimate need acknowledged by the user's immediate Hopkins' superior, either a department head, dean, or office of the Provost, as the case may be. Legitimate users of such material must also use reasonable precautions to prevent the inadvertent viewing of such images by unsuspecting persons who may be offended by such material, or which may constitute sexual harassment or create a hostile work environment.

9. Illegal Acts. Use of IT resources for any illegal purpose is prohibited.

10. Copyright Violations. Transmission of copyrighted materials in violation of U.S. or other copyright laws is prohibited. Hopkins complies fully with the Digital Millennium Copyright Act, and will terminate the access of copyright violators to Hopkins IT resources in accordance with that Act.

a. Copyright exists in any original work which exists or is fixed in any tangible medium of expression. Images displayable on computer screens, computer software, music, books, magazines, scientific and other journals, photographs, and articles are some examples of property to which copyright applies. A copyright notice is not required.

b. Duplication or other copying or distribution of copyrighted materials without permission of the owner or the copyright holder is a violation of federal law, subjects the person initiating the activity to civil and criminal penalties, and exposes Hopkins to claims for damages. Although certain limited copying may be permitted if it is "fair use," what constitutes "fair use" is not always clear. Assistance from Hopkins libraries or the office of General Counsel is recommended.

	The Johns Hopkins Health System	<i>Policy Number</i>	SYS031
	PFS Policies and Procedures Manual	<i>Effective Date</i>	6-4-01
	<i>Subject</i>	<i>Page</i>	8 of 10
	Computer Software Policy	<i>Revised</i>	08-12-05

G. Special Circumstances.

1. Computer Programs. Hopkins provides many programs and data sources which have been obtained under contracts or licenses stating that they may not be copied, cross-assembled, or reverse-compiled. A user is responsible for determining whether or not programs or data are restricted in this manner before copying, cross-assembling, or reverse-compiling them in whole or in part. No unauthorized software should be placed on any Hopkins computer unless a proper license for that software is obtained.

2. Broadcast Messages. Broadcast messages, which are messages sent simultaneously to a specified entire segment of the Hopkins user base, should be used only by those persons specifically authorized to distribute such messages. Individual users should limit group messages to specific and finite recipient lists.

H. Security and Confidentiality.

1. Confidentiality. The confidentiality of electronic mail or other transmissions across any network cannot be assured. Such confidentiality may be compromised by:


- Applicability of law or policy, including this Policy;
- Unintended redistribution of E-mail;
- Transmission of unencrypted data across public network connections; or
- Inadequacy of current technologies to protect against unauthorized access.

2. Hopkins Intellectual Property and Confidential Information. Because security cannot be guaranteed on any network, proprietary, sensitive or confidential information should not be transmitted across Hopkins' networks unless encrypted using approved encryption methods.

3. Encryption. Only authorized encryption tools may be used to encrypt E-mail or establish a digital signature. All such tools must implement key-recovery or key-escrow techniques to permit Hopkins to access and recover encrypted information (e.g., in the case of the absence of the employee who performed the encryption). Encryption tools must be used in compliance with federal law regarding access by non-citizens or use outside the United States. In addition, those planning to use encryption must contact Hopkins Information Technology Services (HITS) for authorization. Hopkins needs in all cases to be able to decrypt all information.

I. Access to computers or messages. When necessary, administrators of Hopkins' IT resources may access users' computers or mail messages without users' prior knowledge or consent. Circumstances in which this is necessary include but are not limited to:

- When required and consistent with law;
- When there is reason to believe that violations of law or of this Policy or any other Hopkins policies have occurred;
- When failure to act may result in bodily harm, property loss or damage, potential loss of evidence of one or more violations of law or of Hopkins policies, or liability to Hopkins or to members of the Hopkins community;
- Under time-dependent, critical operational circumstances where failure to act

	The Johns Hopkins Health System	<i>Policy Number</i>	SYS031
	PFS Policies and Procedures Manual	<i>Effective Date</i>	6-4-01
	<i>Subject</i>	<i>Page</i>	9 of 10
	Computer Software Policy	<i>Revised</i>	08-12-05

- could impair the ability of Hopkins' IT services to continue functioning;
- When IT services have malfunctioned.
- As necessary to protect Hopkins IT resources or perform network services.

J. E-mail and Records Retention.

1. Backups. Users of IT resources should be aware that even though the sender and recipient have discarded their copies of an electronic mail record, there are likely to be backup copies of both the message and attached files that can be retrieved. Computer systems may be backed up on a routine or occasional basis to protect system reliability and integrity, and to prevent potential loss of data. The backup process results in the copying of data onto storage media that may be retained for periods of time and in locations unknown to the originator or recipient of electronic mail. The practice and frequency of backups and the retention of backup copies of E-mail vary from system to system.

2. Records Retention. System backup is distinct from records retention. If E-mail messages or files transmitted over IT resources are needed for future reference, or are required to be preserved by law or agreement, they should be saved locally rather than being stored on central systems.


3. Archives. Hopkins does not maintain central or distributed archives of all electronic mail sent or received. Electronic mail is normally backed up, if at all, only to assure system integrity and reliability, not to provide for future retrieval.

K. Policy Violations.

1. Termination of use privileges. Those who use Hopkins IT resources are expected to do so responsibly, to comply with state and federal laws, and with this and other policies and procedures of Hopkins, as pertain to each division, and with normal standards of professional and personal courtesy and conduct. Access to Hopkins IT resources, when provided, is a privilege that may be wholly or partially restricted by Hopkins without prior notice and without the consent of the computer user when required by and consistent with law, when there is reason to believe that violations of this policy or law have taken place, or, in exceptional cases, when required to meet time-dependent, critical operational needs..
2. Discipline. Violations of Hopkins' policies governing the use of Hopkins IT resources may result in disciplinary action, up to and including dismissal, as may be applicable under this or other Hopkins policies, guidelines, implementing procedures, or collective bargaining agreements.

II. Reference.

- Electronic Communications Privacy Act of 1989, United States code Annotated, Title 18, Crimes and Criminal Procedure, Section 2510
- The Johns Hopkins Human Resources Employee Relations Manual, Section 9: Standards of Conduct and Performance

	The Johns Hopkins Health System	<i>Policy Number</i>	SYS031
	PFS Policies and Procedures Manual	<i>Effective Date</i>	6-4-01
	<i>Subject</i>	<i>Page</i>	10 of 10
	Computer Software Policy	<i>Revised</i>	08-12-05

- The Johns Hopkins Medical Institution Internetwork Service Terms of Service
- The Johns Hopkins Applied Physics Laboratory Standards of Ethics and Conduct

III. Responsibilities.

Hopkins recognizes that each of its Divisions and Campuses operates independently, and a central IT appropriate use policy best serves the Hopkins community by establishing general guidelines. Each Division and Campus may develop, maintain, and publish specific procedures and practices that implement this Policy, according to the academic and business needs of each Division and Campus.

IV. Sponsor.

The sponsor is the Johns Hopkins University Chief Information Officer and Vice Provost for Information Technology/Johns Hopkins Health System Chief Information Officer and Vice President for Information Services.

V. Review Cycle.

This policy will be reviewed one year after its approval date. This policy may be amended at any time, as needed, due to such events as changes in laws, regulations, or technological requirements.

VI. Approval.

This policy was approved by _____ on _____ (date). The policy takes effect on _____ (date).