

Title: Acceptable Use  
Policy Area: Security  
Sub Section: Use

## 1.0 Purpose

Use of the Johns Hopkins Bloomberg School of Public Health (JHSPH) information technology (IT) resources is a privilege that is extended to users for the purpose of accomplishing the school's mission. This privilege comes with the responsibility of using IT resources in a manner consistent with the values and culture of JHSPH. The purpose of this policy is to govern the use of JHSPH IT resources as they apply to promoting a positive image of the school, creating a productive work place, and protecting JHSPH and its employees from disruptive or illegal activities.

## 2.0 Scope

This policy applies to all users of the JHSPH IT resources. Users include but are not limited to faculty, visiting faculty, staff, students, vendors, and consultants. IT resources are the devices, infrastructure, applications and data, including resources designated for the use of a single individual, that comprise the JHSPH computer network and are the sole property of JHSPH.

Furthermore, JHSPH owns all network traffic that traverses its infrastructure (though not necessarily the content of that traffic), regardless of the source of the traffic. To understand this concept, think of the US Postal Service. Once a letter is dropped in a mailbox the Postal Service owns the letter until it is delivered. Even the original sender cannot reclaim the letter. However, the sender still maintains copyright ownership of the content of that letter.

## 3.0 Background

The topics covered by this policy involve a wide variety of issues. They can be roughly summarized by three guiding principles:

- Do nothing illegal
- Do nothing to harm JHSPH
- Respect your coworkers

## 4.0 Policy Statement

### Illegal Activity

JHSPH IT resource may not be used for any illegal activity as defined by local, state, federal or international law. All legal questions should be directed to the Office of General Counsel. Examples of illegal activity include, but are not limited to the following:

1. Posting or disseminating material that is unlawful such as child pornography.
2. Pyramid or other illegal soliciting schemes.
3. Fraudulent activities, including impersonating any person or entity or forging anyone else's digital signature.

4. Harassment or threats of any kind. Examples include but are not limited to:
  - Distribution of offensive material
  - Repeated unwelcome contact
  - Words, phrases or statements that would create a hostile work environment. This includes, but is not limited to, racially, ethnically or sexually offensive language.
5. Unauthorized access of or prevention of authorized access to systems outside the JHSPH domain. This includes, but is not limited to:
  - Accessing data not intended for you
  - Logging into or making use of a server or account you are not expressly authorized to access
  - Probing the resources or security of other networks
  - Denial of service attacks
6. Any use of materials in violation of intellectual property laws such as copyright laws or of vendor licensing agreements. JHSPH complies fully with all local, state and federal intellectual property laws, including the Digital Millennium Copyright Act.

### **Activity Harmful to JHSPH**

JHSPH IT resources may not be used for activities that would be harmful to the legal status or reputation of JHSPH. User may not participate in activities that prevent the use or unduly degrade the performance of JHSPH IT resources. Examples of these activities include but are not limited to the following:

1. Use inconsistent with non-profit status of JHSPH
  - 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-JHSPH business purposes is prohibited. Communication and exchange of data that may have an incidental commercial benefit to an external organization are permitted, so long as it furthers the JHSPH mission.
2. Participation in activities that cause excessive strain on or interfere with the use of JHSPH IT resources. Examples include, but are not limited to:
  - Distributing unsolicited bulk email
  - Transferring multiple or large files
  - Performing network scanning
  - Attaching to external sites for the purpose of accessing non-JHSPH work related video and audio streams
3. Intentionally distributing, using or allowing propagation of any malicious software. Malicious software are programs or scripts that seeks to damage, propagate, deny use, allow unauthorized access or transmit unauthorized data to or from any JHSPH resource. Examples of malicious software include but are not limited to:
  - Viruses or Worms
  - Rootkits, Backdoors or Trojans
  - DoS (Denial of Service)
  - Programs or scripts that cause buffer overflow
  - Password guessing/cracking programs

---

**NOTE:** Department of Information Systems users engaged in JHSPH-sanctioned malicious software research must take appropriate precautions to isolate the research systems from general JHSPH IT resources to prevent accidental distribution or data release.

4. Personal use that has an undue impact on the operation of JHSPH IT resources. Occasional, limited, personal use of the JHSPH IT resources is permitted if it meets the following criteria:
  - The use does not adversely effect JHSPH IT resources
  - The use does not violate any other provision of this policy or any other policy, guideline or standard of JHSPH
  - The use does not violate any applicable Local, State, or Federal Laws

**NOTE:** At all times, users have the responsibility to use the JHSPH IT resources in a respectful, professional, ethical, and lawful manner.

5. Broadcasting information or messages. This includes, but is not limited to, sending mass e-mail and broadcasting instant messenger messages. Legitimate mass-mailings should use one of the Listserv addresses and be sent only by authorized users.

#### **Activity Contrary to the Values of JHSPH**

Use of JHSPH IT resources must reflect the following values:

- Respect for others
- Civil discourse
- Forthright communication

JHSPH reserves the right to refuse to post or to remove any electronic information or materials that it deems, at its sole discretion, to be offensive, indecent, fraudulent or otherwise inappropriate regardless of whether such material or its dissemination is lawful. Examples of activities that do not reflect the institutions values include but are not limited to:

1. Attempting to access a JHSPH IT resource for which a user is not authorized. Availability of a resource does not imply authorization. Simply because a particular resource has open access does not mean everyone who has access is authorized to use the resource. Examples of attempted access include but are not limited to:
  - Trying different user names and passwords at login screens
  - Exploring open file shares
  - Using a workstation logged-in under another users account
2. Attempting to conceal your identity, masquerading or impersonating another user or adopting a false identity when using any JHSPH IT resource.
3. Selling or proselytizing for commercial ventures, religious causes or political campaigns, outside organizations or other non-JHSPH related activities without specific prior authorization from the receiver of the message. Examples of where this activity is prohibited include but are not limited to:
  - Unsolicited e-mail
  - E-mail signature files
  - Computer screen savers and desktop backgrounds

4. Using JHSPH IT resources to solicit funds or donations for any organization including both JHSPH and non-JHSPH concerns without prior approval from either the recipient or the specific JHSPH organization delegated to review and approve solicitations. This includes, but is not limited to:

- Both commercial and non-commercial ventures
- Churches or religious activities
- Political campaigns or causes

All forms of Internet and intranet communications are covered by this prohibition. The forms of communications include but are not limited to:

- E-mail, especially unsolicited e-mail without the recipients prior approval
- Chat or Internet Messaging (IM)
- IP telephony, including but not limited to programs such as Skype

5. Using JHSPH IT resources to send, store or display material that is sexually explicit, intimidating, defamatory, discourteous, offensive or otherwise inappropriate.

6. Using e-mail signature files that contain information other than what is necessary for identification and contact. For example, inspirational quotes and personal expressions are inappropriate.

7. Using JHSPH resources to transmit, view or download sexually explicit content except as may be necessary and appropriate for legitimate medical, scholarly or forensic purposes. If there is a legitimate need to access such material using JHSPH IT resources, disclosure of the need and the type of material to be accessed shall first be made to the user's supervisor. If access has been blocked the user's supervisor will contact Information Systems and request that access be given. Legitimate users of such material must take reasonable precautions to prevent the exposure of this content to others.

## 5.0 Enforcement

JHSPH IT resources are acquired and implemented by JHSPH to assist users in the performance of their jobs. Users should not have an expectation of privacy in anything they create, store, send, or receive using those resources. Email and user accounts and their contents are generally considered private, but neither policy nor technology is able to guarantee privacy. Files stored on JHSPH IT resources are presumed to be the property of JHSPH, and there can be no expectation of privacy concerning such files stored on or transmitted across JHSPH IT resources. For safety and/or legal purposes, or as needed to maintain or protect its facilities, JHSPH reserves the right to copy, examine and disclose all email messages and files stored on any institution-owned media or equipment, or transmitted across or through JHSPH network facilities.

All network traffic, regardless of the source, will be monitored as necessary. Reasons for monitoring include but are not limited to the following:

- Maintaining the integrity and performance of JHSPH IT resources.
- Enforcement of JHSPH policy.
- Compliance with local, state and federal law or their agents.

The Johns Hopkins Bloomberg School of Public Health has no obligation to monitor the network for violations of acceptable use. An absence of monitoring in no way limits its right to monitor all network traffic.

The Information Systems Assistant Director of Operations (ISADO) is responsible for ensuring adequate monitoring technology is in place wherever possible to enforce specific

provisions in this policy. In many cases, however, JHSPH must rely on a concerned and alert user community to report violations. The Information Systems Security Officer (ISSO) reviews e-mail sent to [isso@jhspg.edu](mailto:isso@jhspg.edu) for reports on violation of the Acceptable Use Policy. Reports are forwarded to the ISADO who is responsible for determining the appropriate enforcement organizations to which violations will be reported.

Violations will be taken seriously and may result in disciplinary action, including possible termination, and civil and criminal liability. Certain violations may constitute criminal activity that may be referred to local, state or federal law enforcement authorities. In particular, Federal statutes 18 USCS 2511 (Electronic Communications Privacy Act), 18 USCS 1030 (Computer Crime Act) and Maryland State statute Article 27, Section 146, deal with the use of information technology and networking. The failure to enforce this Policy, for whatever reason, shall not be construed as a waiver of any right to do so at any time.

## 6.0 Actions

This policy is effective June 1st, 2003.

## 7.0 Responsibility for Policy Maintenance

It is the responsibility of the ISSO to ensure that this policy is current and relevant. The ISSO must review this policy every 5 years from the date the policy becomes effective and submit any changes for approval to the Director of Information Systems

Policy is due for review June 1st, 2008.

## 8.0 Authority

Authority for this comes from the office of the Dean of The Johns Hopkins Bloomberg School of Public Health.

## 9.0 Revision History

Initial policy approved by Director of Information Systems May 16th, 2003.

On July 6<sup>th</sup>, 2006, the following point in the Activity Contrary to the Values of JHSPH section was changed from:

3. Soliciting or proselytizing for commercial ventures, religious causes or political campaigns, outside organizations or other non-JHSPH related activities without specific prior authorization from the receiver of the message. Examples of where this activity is prohibited include but are not limited to:
  - Unsolicited e-mail
  - E-mail signature files
  - Computer screen savers and desktop backgrounds

To:

3. Selling or proselytizing for commercial ventures, religious causes or political campaigns, outside organizations or other non-JHSPH related activities without specific prior authorization from the receiver of the message. Examples of where this activity is prohibited include but are not limited to:
  - Unsolicited e-mail
  - E-mail signature files
  - Computer screen savers and desktop backgrounds

On July 6<sup>th</sup>, 2006, the following point was inserted into Activity Contrary to the Values of JHSPH section as point 4.:

4. Using JHSPH IT resources to solicit funds or donations for any organization including both JHSPH and non-JHSPH concerns without prior approval from either the recipient or the specific JHSPH organization delegated to review and approve solicitations. This includes, but is not limited to:
  - Both commercial and non- commercial ventures
  - Churches or religious activities
  - Political campaigns or causes

All forms of Internet and intranet communications are covered by this prohibition. The forms of communications include but are not limited to:

- E-mail, especially unsolicited e-mail without the recipients prior approval
- Chat or Internet Messaging (IM)
- IP telephony, including but not limited to programs such as Skype

The policy revisions dated July 6<sup>th</sup>, 2006 were approved by Director of Information Systems July 11, 2006.