

Institute for Medical Research, Inc.	Policy on Computer, Internet & E-mail Usage	No. 506	
		Effective Date 4/14/09	
		Revision Date	
		Final Approval	Approved by IMR Board of Directors: 4/14/09

Purpose

To establish IMR's policy on computer internet and e-mail usage.

Scope

IMR employees and Investigators

Policy

Internet access to global electronic information resources on the World Wide Web is provided to assist employees in obtaining work-related data and technology. The following guidelines have been established to help ensure responsible and productive Internet usage.

All Internet data that is composed, transmitted, or received via our computer communications systems is considered to be part of the official records of IMR and/or the VA and, as such, is subject to disclosure to law enforcement or other third parties. Consequently, employees should always ensure that the business information contained in Internet e-mail messages and other transmissions is accurate, appropriate, ethical, and lawful.

The equipment, services, and technology provided to access the Internet remain at all times the property of IMR. As such, IMR reserves the right to monitor Internet traffic, and retrieve and read any data composed, sent, or received through our online connections and stored in our computer systems. Employees should not use a password, access a file, or retrieve any stored communication without authorization.

Data that is composed, transmitted, accessed, or received via the Internet must not contain material that could be considered discriminatory, offensive, obscene, threatening, harassing, intimidating, or disruptive to any employee or other person. Examples of unacceptable content may include, but are not limited to, sexual comments or images, racial slurs, gender-specific comments, or any other comments or images that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.

The unauthorized use, installation, copying, or distribution of copyrighted, trademarked, or patented material on the Internet is expressly prohibited. As a general rule, if an employee did not create material, does not own the rights to it, or has not obtained authorization for its use, it should not be put on the Internet. Employees are also responsible for ensuring that sending any material over the Internet has the appropriate distribution rights.

Abuse of the Internet access provided, in violation of law or IMR policies will result in disciplinary action, up to and including termination of employment. Employees may also be held personally liable for any violations of this policy. The following behaviors are examples of previously stated or additional actions and activities that are prohibited and can result in disciplinary action:

- * Sending or posting discriminatory, harassing, or threatening messages or images
- * Using the organization's time and resources for personal gain
- * Stealing, using, or disclosing someone else's code or password without authorization
- * Copying, pirating, or downloading software and electronic files without permission
- * Sending or posting confidential material, trade secrets, or proprietary information outside of the organization
- * Violating copyright law
- * Failing to observe licensing agreements
- * Engaging in unauthorized transactions that may incur a cost to the organization or initiate unwanted Internet services and transmissions
- * Sending or posting messages or material that could damage the organization's image or reputation
- * Participating in the viewing or exchange of pornography or obscene materials
- * Sending or posting messages that defame or slander other individuals
- * Attempting to break into the computer system of another organization or person
- * Refusing to cooperate with a security investigation
- * Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities
- * Using the Internet for political causes or activities, religious activities, or any sort of gambling
- * Jeopardizing the security of the organization's electronic communications systems
- * Sending or posting messages that disparage another organization's products or services
- * Passing off personal views as representing those of the organization
- * Sending anonymous e-mail messages
- * Engaging in any other illegal activities

Employees should notify their immediate supervisor, the IMR Administrative Office or an appropriate member of management upon learning of violations of this policy. Employees who violate this policy will be subject to disciplinary action, up to and including termination of employment.