

NAVOPMEDINST INSTRUCTION 5230.5

Subj: USE OF THE INTERNET AND INTRANET

Ref: (a) DOD Directive 5500.7-R, Joint Ethics Regulations  
(b) SECNAVINST 5216.5D  
(c) NOMIINST 5230.4C  
(d) CINCPACFLT/CINCLANTFLT 210151Z Feb 98  
(e) Office of the Assistant Secretary of Defense  
(Health Affairs) Policy Document 97-064

1. Purpose. Following the guidelines of references (a) through (e), this instruction provides policies on the use of the Internet and Intranet on government computers at the Naval Operational Medicine Institute (NOMI). Violations of the prohibited activities listed in paragraphs 4f(1) through 4f(15) of this instruction are subject to administrative and/or disciplinary action, including non-judicial punishment or court-martial. This is a new instruction and should be read in its entirety.

2. Scope. This instruction applies to the NOMI Headquarters, its detachments and components.

3. Background. The Internet, specifically the World Wide Web, is a public network for obtaining and disseminating information worldwide. The Intranet is a private network of computers within the NOMI domain. The Internet and Intranet provide users with access to information resources that enable them to perform their jobs efficiently and completely. With the privilege of utilizing these resources comes the responsibility to use them in an acceptable fashion. The Internet and Intranet are shared resources and as such require users to conduct themselves in an ethical and acceptable manner.

4. Policy

a. Per reference (a), the Internet and Intranet are primarily for official use and authorized purposes only. The Internet possesses the power to disseminate information world wide instantaneously. Therefore, publishing information and correspondence via the World Wide Web will be in accordance with reference (b).

07 Mar 01

b. The purpose of the Intranet is to provide command-related information to users within the NOMI network domain. Publishing information on the intranet will be managed by the command Webmaster in the Management Information Department. Competent authority will publish information on the Intranet.

c. Access to both the Internet and Intranet at NOMI is a privilege and not a right of employment. Therefore, Internet and Intranet privileges may be denied in part or in entirety, as directed by the Commanding Officer.

d. Per reference (a), government computers, networks, and facilities are government property and not personal property, and the use of government communications systems, including the use of the Internet, is subject to monitoring, interception, accessing, and recording, and may be passed to law enforcement agencies. Therefore, all users of the Internet on government computing systems have no expectation of privacy or confidentiality.

e. Permissible Uses of the Internet and Intranet. The Internet and Intranet may be used for personal purposes per reference (a), as long as such use:

(1) Does not adversely affect the performance of official duties.

(2) Does not overburden NOMI's computing resources or network communication systems.

(3) Does not adversely reflect upon the Department of Defense, Department of the Navy, the Navy Medical Department, or NOMI, Pensacola (to include viewing and transmitting pornographic materials; racial, ethnic, sexist, and indecent/obscene jokes and literature; chain letters; unofficial advertising; and inappropriately handled classified information).

f. Prohibited Uses. The use of the Internet and Intranet on government computer resources is prohibited for purposes other than those described in paragraphs 4e(1) through 4e(3) above. Examples of prohibited use include, but are not limited, to the following:

(1) Introducing classified information into an unclassified system or environment.

(2) Accessing, storing, processing, displaying, distributing, transmitting, or viewing material that is pornographic, racist, promotive of hate crimes, or subversive in nature.

(3) Storing, accessing, processing, or distributing classified, proprietary, sensitive, For Official Use Only (FOUO), or Privacy Act protected information in violation of established security and information release policies.

(4) Obtaining, installing, copying, pasting, transferring, or using software or other materials obtained in violation of the appropriate vendor's patent, copyright, trade secret, or license agreement.

(5) Knowingly writing, coding, compiling, storing, transmitting, or transferring malicious software code, to include viruses, logic bombs, worms, and macro viruses.

(6) Promoting partisan political activity.

(7) Disseminating religious materials outside an established command religious program.

(8) Using the system for personal financial gain, such as advertising or solicitation of services or sale of personal property, with the exception of utilizing a command-approved mechanism such as a Morale, Welfare, and Recreation (MWR) electronic bulletin board for advertising personal items for sale.

(9) Fund-raising activities, either for profit or non-profit, unless the activity is specifically approved by the command (e.g., MWR car washes).

(10) Gambling, wagering, or placing of any bets.

(11) Writing, forwarding, or participating in chain letters.

(12) Posting personal home pages.

(13) Participation in chat rooms for uses other than those outlined in paragraphs 4e(1) through 4e(3).

(14) Personal encryption of electronic communications.

(15) Plagiarism; cutting and pasting ideas from the Internet into your own document without giving credit to the author.

g. Punitive Nature. Any violations of the prohibited uses, as delineated above, are subject to disciplinary and/or administrative action.

5. Action

a. Directors, Department Heads, Division Officers

(1) Ensure policy guidelines contained in this instruction are followed.

(2) Control and monitor access and usage within respective directorate/department/division.

(3) Conduct preliminary inquiry on any unauthorized Internet and Intranet use and, where warranted, hold individuals accountable for unauthorized or inappropriate Internet access.

b. Head, Information Management/Technology Department and Information Systems Security Manager

(1) Monitor local network usage and take appropriate action as directed by competent authority, when inappropriate use is suspected.

(2) Investigate any unauthorized Internet and Intranet uses.

c. Network Security Manager

(1) Monitor network utilization to ensure processing and network resources are not adversely impacted by Internet use, with specific attention being placed on Internet applications and services which are band-width intensive and have a detrimental effect on telecommunications infrastructure.

NOMIINST 5230.5  
07 Mar 01

(2) Configure links on computerized workstations to  
access the Intranet.

/s/

J. H. FAHEY

Distribution:  
List A