

20 Aug 98

FLEET TRAINING CENTER SAN DIEGO INSTRUCTION 5230.2

Subj: INTERNET ACCESS, E-MAIL POLICY AND USE OF GOVERNMENT-OWNED INFORMATION SYSTEMS

Ref: (a) DOD DIRECTIVE 5500.7-R  
(b) CNETINST 5230.9B  
(c) ALPACFLT 003/98 ALLANTFLT 006/98  
(d) OPNAVINST 5239.1A

1. Purpose. To establish policy concerning Internet access and use of individual E-mail on Fleet Training Center information systems.

2. Background. The Department of Defense and Department of the Navy are in the midst of what has been referred to as an information explosion. The exponential growth of the Internet and World Wide Web (WWW) improves many facets of our operations, and provides an efficient and effective means of communication and information distribution. Proficiency in the use of personal computers and computer networking, including use of the Internet, is a requirement for all hands to accomplish FTC's mission. Additionally, to accomplish a responsive, paperless office environment using E-mail communications, policies and procedures must be established and followed.

3. Scope. This instruction addresses Internet access, e-mail and use of government-owned information systems by staff, students, contracted personnel and sub-tenant organizations with access to the FTC LAN.

4. Responsibility. Compliance with this instruction is the responsibility of all personnel assigned to Fleet Training Center, San Diego, as well as personnel utilizing its information system. The Head, Information Systems (N25) is responsible for contents of this instruction.

5. Policy. Consistent with legal and security rules described below, Fleet Training Center personnel, military and civilian, are encouraged to use their government computers to access the Internet and develop their information skills. FTC personnel will have access to e-mail and the Internet through the Local Area Network (LAN).

20 Aug 98

The best way to develop information technology skills is to get on the Internet and make it the preferred and routine choice to access, develop and exchange information. This includes, but is not limited to, accessing the Internet, browsing the World Wide Web and communicating via e-mail. Permissible uses are defined to include all uses not prohibited by law, regulation, instruction or policy described herein. Prohibited uses include:

a. Introducing classified information into an unclassified system or environment. FTC's LAN is an unclassified system.

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

c. 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.

d. 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.

e. Knowingly writing, coding, compiling, storing, transmitting or transferring malicious software codes, to include viruses, logic bombs, worms and macro viruses.

f. Promoting partisan political activity.

g. Disseminating religious materials outside an established command religious program.

h. Using the system for personal financial gain, such as advertising, solicitation of services or sale of personal property.

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

20 Aug 98

- j. Gambling, wagering or placing of any bets.
  - k. Writing, forwarding or participating in chain letters.
  - l. Posting personal home pages.
  - m. Personal encryption of electronic communications.
6. Personal software will not be loaded onto government-owned information systems without authorization from the Head, Information Systems Department. This includes programs used to access the internet such as America On-line or Prodigy.
7. Installation and use of modems on government-owned information systems is prohibited unless authorized by the Head, Information Systems Department.
8. All users are reminded that they have no expectation of privacy in the use of government information systems. Use of government information systems, including use of the Internet and e-mail, is subject to monitoring, interception, accessing and recording, and may be passed to law enforcement. Any violation of this instruction can result in disciplinary or administrative action.
9. Internal e-mail capabilities will be used, where possible, to route and review correspondence, word processing documents (letters, reports, messages), graphics and spreadsheet packages. E-mail is not intended to be a filing system. Personnel will actively manage their e-mail accounts to minimize the number of messages stored on the LAN.
10. Maintenance and adherence to post office directory and e-mail naming conventions will be in accordance with reference (b) and will be the responsibility of the e-mail administrator.
11. Use of government information systems including e-mail and Internet access may be controlled or limited for purposes of security, morale, good order and discipline, or to promote efficiencies of the command. For example, access to specific sites may be purposely blocked, Internet access limited or an individual's use of e-mail could be revoked altogether. Similarly, limits may be placed on the size and type of electronic files that can be downloaded, so as to prevent the system from being overburdened.

FLETRACENSINST 5230.2

20 Aug 98

12. The foregoing policy will directly improve the professional skills of our personnel, enhance productivity and, most importantly, support our mission by ensuring that we have timely access to all available information.

C. E. MULROY

Distribution: (FLETRACENSINST 5400.1N)

List 1a, b, c, d