



UNITED STATES MARINE CORPS
MARINE CORPS BASE
QUANTICO, VIRGINIA 22134-5001

IN REPLY REFER TO:

5230

B 37

AUG 05 2010

From: Director, Marine Corps Community Services Division,
Marine Corps Base Quantico

To: All Personnel having Internet Access

Subj: INTERNET ACCESS AND ELECTRONIC MESSAGING

Ref: (a) MCBO 5230.3
(b) MARADMIN 162/00

1. Marine Corps Enterprise Network (MCEN) which interconnects Marine Corps commands and activities provides Information Technology (IT) Resources that include, but are not limited to: computer hardware and software, telecommunications infrastructure (desktop and wireless phones), local area networks, facsimile machines, electronic mail (e-mail) and internet access to MCCA staff members who have demonstrated a need pursuant to the execution of their official work duties.

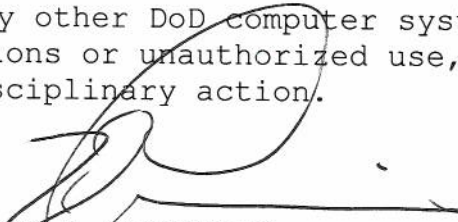
2. Staff members who use this Internet access are reminded that system monitoring is in progress through periodic audits as outlined in MARADMIN 162/00, to include but not limited to; accessing/logging into commercial e-mail services via web interface (e.g., hotmail.com, aol.com, att.net, etc.) from within MCEN; commercial activities for personal financial gain (sales) and uses which reflect adversely on DoD (EEO violations, extremist organizations, sexist activity, harassment). Furthermore, under no circumstances will official government correspondence or data files be sent or forwarded to, created or stored on commercial e-mail services (web enabled or otherwise).

3. Use of network services (internet access and e-mail) provided by or through the installations IT department affirms consent to monitoring. Staff members who are found to be in violation of these rules will have Internet and/or e-mail access revoked indefinitely and the incident reported to their supervisor.

4. All DoD computer systems and related equipment are for communication; transmission, processing and storage of official U.S. government or other authorized information only. Those systems are subject to monitoring at all times to insure proper functioning of equipment and systems to include security devices, to prevent unauthorized use and violations of statutes

or security regulations, to deter criminal activity, and for other similar purposes. All users should be aware that any information placed in the computer system is subject to monitoring and is not subject to any expectation of privacy. If monitoring of this or any other DoD interest computer system reveals possible evidence of violation of criminal statutes, this evidence and any other related information, including identification information about the user, may be provided to law enforcement officials.

5. If monitoring of this or any other DoD computer system reveals violation of security regulations or unauthorized use, employees are subject to appropriate disciplinary action.



T. E. LOUGHLIN

I have read and understand this document for compliance.

Print Employee Name

Employee Signature

Date

Copy to: OPF