

Minnesota National Guard Web Log Policy

1. References:

- a. [DoD 5230.9](#), Clearance of DoD Information for Public Release, 9 APR 96
- b. [AR 25-1](#) Army Knowledge Management and Information and Information Technology Management, 30 JUN 04.
- c. [AR 25-2](#), Information Management, 14 NOV 03.
- d. [AR 360-1](#), The Public Affairs Program, 15 SEP 00

2. Purpose. This policy provides general guidance and operational policy for unit and Soldier/Airmen owned and maintained websites. It applies to currently owned and maintained websites or plans for future purchases or leases of websites.

3. Applicability. This policy applies to all Minnesota National Guard Soldiers and Airmen, civilians, and contractors assigned to or working for the Minnesota National Guard.

4. Definitions:

a. Official websites. Any website listed in the “.mil” domain, or in the case of Minnesota, the “.state.mn.us” domain. “<http://www.MinnesotaNationalGuard.org> is an alias that is ran by the “state.mn.us” server. These Websites are created and maintained as part of official duties and paid for with appropriated funds.

b. Unofficial Websites. These Websites are created on personal time, and are not produced in connection with military duties, and are not paid by DoD funds.

c. Web log or “blog.” This refers to a Web page maintained as a journal for personal comments. It may include photos, video, audio or hyperlinks to other web pages.

d. Uniform Resource Locator (URL). This refers to the web address of the website.

e. Army Web Risk Assessment Cell (AWRAC). A team of information assurance personnel that conduct ongoing operational security and threat assessments of Army publicly available web sites to ensure compliance with DoD and Army policy and best practices.

f. Webmaster. This refers to the individual who maintains the web page, portal, or site.

g. Official Information. All information that in the custody and control of DoD, relates to information in the custody and control of DoD, or was acquired by DoD employees as a part of their official duties or status.

h. Prohibited information. Any official information that is generally not available to the public and which would not be released.

5. Minnesota National Guard personnel owning or desiring to maintain a unit or individual website or blog must be registered with their chain of command. Lists will be maintained by the JFHQ PAO.

6. **BLOGGING Guidance and proposed DoD Policy**

Throughout American history our service members have been the most credible, influential and authentic spokespersons for the U.S. military way of life. Their diaries, letters and handwritten journals have provided some of the clearest accounts and most authentic historic documentation of America’s battles and warfare. But, the age of handwritten, diaries, journals and letters is all but gone. They are being replaced by instantaneous worldwide communication.

Rather than diminishing the personal record of events and military life, this new form of interaction has greatly advanced the service member's ability to communicate.

Internet home pages, message boards, Web Logs (BLOGS), Web-based Video Diaries (VLOGS) and other Internet video products, standard email, wireless text messaging and other evolving forms of electronic media have become increasingly popular as a convenient means for service members to communicate in real and near-real time with families, friends and the general public - nationally and internationally.

The most prolific form of such media currently is the Web Log or "BLOG", which is a frequently updated, simple web site highlighted by personal commentary, editorial comments, and regularly links to supporting web sites. Often a personal journal, BLOG consists of dated entries in chronological order, and invites and/or permits comments from readers.

BLOGS and other emerging forms of communication are proliferating the Internet at unprecedented, even alarming rates. Though generally created for personal use, they are often used by advocacy groups or people with recognized or self-proclaimed expertise in a particular subject. Consequently, they have become sources of information for the traditional news media as well as the public at large.

Military and civilian personnel, especially when deployed overseas or in situations where usual civilian communication channels are limited, are using BLOGS to communicate with family and friends. But, Web logs, or BLOGS, and other personal diaries, including video products are open to review by anyone with World Wide Web access. Uninformed users often think of these mediums as tools for conversation amongst peers, but, because of the public nature of BLOGS, they are open to unlimited view and dissemination.

BLOGS and OPSEC

With the increased speed and capability of these digitized and wireless communications comes increased personal and military unit responsibility. As easily as service members can text message, e-mail, or post information to a web log (BLOG), Web-based Video Diary (VLOGS) or other evolving forms of electronic media or video invention, our adversaries can retrieve and monitor these sources. Information harvested here has the potential to make our adversaries much more lethal.

All Department of Defense (DOD) personnel must understand that whether classified or unclassified the information to which they have access including their very life style is valuable to our adversaries.

Before posting or transmitting information ask yourself if you are about transmit information that could be helpful to the enemy. Be responsible when describing daily activities, experiences, locations, or places. Comply explicitly with the protection and operational security policies of the Department of Defense.

BLOG Guidance

Government provided information and communication systems are for official use and authorized purposes only. Authorized purposes may include limited personal use when permitted by commanders/commanding officers and supervisors for morale and welfare purposes, but, whether accessed at home or at work, OPSEC training and education apply to electronic communication just as it does to personnel conversations, correspondence, and telephone conversation. DOD policies against communicating with unauthorized personnel apply just as strictly to electronic communication such as BLOGS.

Always assume the entire world, adversaries included, is reading or intercepting your material – email, BLOG, or personal web page, text message, or video transmission.

The American military is a values-based organization; DOD employees including service members, civilians and contractors represent that organization. Before writing or posting anything, consider whether or not the information appropriately represents and conveys American values.

All information (including personal information) placed on or sent over DOD computer systems may be monitored. E-mail, personal user files and directories, and any use of the Internet or records created by Internet use or other government supplied electronic devices are subject to monitoring, inspection, and audit by command or agency management or its representatives at any time, with or without notice. The use of DOD computer systems legally implies that the user consents to monitoring and understands that the command or agency has the right to inspect and audit all information, including e-mail communications and records created by Internet use

Any official DOD information (any communication or representation of knowledge such as facts, data, or opinions in any medium or form) intended for public release that pertains to military matters, national security issues, or subjects of significant concern to the Department of Defense shall be reviewed for clearance by appropriate security review and Public Affairs Officers prior to release per DOD Directive 5230.9 (para 4.2)

Personal websites and web logs or BLOGS produced in a personal capacity and not in connection with official duties or with government supplied equipment restricted from such use, require no advance clearance. However, it is the personal responsibility of service members and DOD employed civilians to ensure that any such electronic communication does not contain un-releasable information as defined in DOD OPSEC training and guidance.

Personnel should also consider adding a disclaimer to personal websites to preclude readers from assuming unofficial sites represent an Official DOD position. Also be aware that the reasonable restrictions on free speech (for example, no political commentary while in uniform) extend to similar restrictions on electronic communications identified by rank or photos in uniform. Personal websites should not contain product endorsements or inflammatory comments. Personnel who have questions regarding prohibited release must seek guidance from their Public Affairs staff.

Additionally, personnel must be sure that no laws or regulations are violated (5230.9 para 4.8.1), that ethical standards are maintained as described by DOD Directive 5500.7 and DOD 5500.7-R

Preparation activities, as explained earlier, are not to be done during normal duty hours or with the use of DOD facilities, property, or personnel except as authorized (see DOD Directive 5230.9 (para 4.8.4.) The author is prohibited from using official DOD information generally not available to the public and which would not be released under DOD 5400.7-R.

The following is a summary of some of the types of information that must not be displayed on any public accessible web site including personal BLOGS or other electronic media operated by individual service members or DOD civilian or contract employees:

- Pre-decisional information, proprietary information, business sensitive information, information designated as For Official Use Only (FOUO).
- Information that is not based on personal experience or not in the scope of personal duties.
- Information protected by the Privacy Act of 1974 or the Health Insurance Portability and Accountability Act (HIPAA) of 1996.

- Information --- other than authorized press releases --- about casualties prior to official confirmation that next of kin have been notified and some competent authority authorizes publication of specific casualty information. Commanders are reminded that casualty information is to be tightly controlled and heavily scrutinized.
- Information --- other than authorized press releases --- regarding events or incidents currently under investigation.
- Information that is under copyright or trademark, without permission of the holder.
- Unit or other personnel lists/rosters, charts or directories, or the names, addresses and telephone numbers of unit members
- Any image, still or motion, of any military operation or activity unless that image is personal and has been cleared by the proper authority.

Finally, remember, once you post information, it cannot be “removed.” Ask yourself, “Is this how I want to be remembered?”

7. The Minnesota National Guard encourages personal websites and blogging. These websites are reviewed on a quarterly basis by the PAO to ensure compliance.

8. Point of contact is JFHQ-PAO at public.affairs@mn.ngb.army.mil