



Office, Chief Information Officer / G-6

DEPARTMENT OF THE ARMY
OFFICE OF THE SECRETARY OF THE ARMY
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

AUG 27 2009

SAIS-GKM

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Use of Social Media Tools

1. The enclosures to this memorandum provide guidance regarding the official and unofficial use of network-based collaborative technologies, also known as social media tools. These technologies, which are further defined in the enclosed glossary include, but are not limited to: blogs; web feeds (Really Simple Syndication (RSS) feeds); social networking sites; video sharing sites; photo and map tags; and wikis. These tools, when utilized properly and responsibly, enhance the exchange of information and improve overall productivity.
2. Social media sites are often deployed in an environment that is not under the Army's direct control. Therefore, protection of sensitive information is the responsibility of the individuals that use these technologies. It is imperative that the security of Army networks be maintained and that OPSEC rules be followed.
3. For more information regarding precautions that must be considered before officially using social media sites, refer to the enclosed "Guidelines for Army Social Media Use" and the memorandum from the Office of the General Counsel which is located at the following link: <https://www.us.army.mil/suite/folder/18595064>.
4. It is anticipated that the Department of Defense will soon release policy regarding the use of social media tools. Army guidance will be updated to reflect overarching DoD policy, as necessary.
5. The Point of Contact is Ms. Amber Pittser, email: amber.pittser@us.army.mil comm: 703-602-0274.

2 Encl


JEFFREY A. SORENSON
Lieutenant General, GS
Chief Information Officer/G-6

SAIS-GKM
SUBJECT: Use of Social Media Tools

DISTRIBUTION:
PRINCIPAL OFFICIALS OF HEADQUARTERS, DEPARTMENT OF THE ARMY

COMMANDER

US ARMY FORCES COMMAND
US ARMY TRAINING AND DOCTRINE COMMAND
US ARMY MATERIEL COMMAND
US ARMY EUROPE AND SEVENTH ARMY
US ARMY CENTRAL
US ARMY NORTH
US ARMY SOUTH
US ARMY PACIFIC
US ARMY SPECIAL OPERATIONS COMMAND
MILITARY SURFACE DEPLOYMENT AND DISTRIBUTION COMMAND
US ARMY SPACE AND MISSILE DEFENSE COMMAND/ARMY STRATEGIC
COMMAND
EIGHTH US ARMY

CF:

COMMANDER

US ARMY NETWORK ENTERPRISE TECHNOLOGY COMMAND/9TH SIGNAL
COMMAND
US ARMY MEDICAL COMMAND
US ARMY INTELLIGENCE AND SECURITY COMMAND
US ARMY CRIMINAL INVESTIGATION COMMAND
US ARMY CORPS OF ENGINEERS
US ARMY MILITARY DISTRICT OF WASHINGTON
US ARMY TEST AND EVALUATION COMMAND
US ARMY RESERVE COMMAND
US ARMY INSTALLATION MANAGEMENT COMMAND

SUPERINTENDENT, US MILITARY ACADEMY
DIRECTOR, US ARMY ACQUISITION SUPPORT CENTER

Army Guidelines for Social Media Use

1. References:

- a. 5 CFR Part 2635, Standards of Ethical Conduct for Employees of the Executive Branch.
- b. Army Regulation 25-1, Army Knowledge Management and Information Technology Management, 4 December 2008.
- c. Army Regulation 25-2, Information Assurance, 23 March 2009.
- d. Army Regulation 25-400-2, The Army Records Information Management System (ARIMS), 2 October 2007.
- e. Army Regulation 360-1, The Army Public Affairs Program, 15 September 2000.
- f. Army Regulation 380-5, Department of the Army Information Security Program, 29 September 2000.
- g. Army Regulation 530-1, Operations Security, 19 April 2007.
- h. DODD 5230.09, Clearance of DOD Information for Public Release, 22 August 2008.
- i. DOD 5500.7-R, Joint Ethics Regulation, 29 November 2007.

2. Army leadership recognizes that the use of official collaborative tools can greatly enhance mission effectiveness; however, it is imperative that OPSEC and Information Assurance (IA) regulations be followed in accordance with Army Regulations 25-2, 530-1, and 380-5. Army personnel must safeguard classified and sensitive information in all online communications and must understand that online communications on the .com are directed at the public. Contacts made through online communications with the public are unverified and therefore should not be trusted.

3. Commanders must maintain up-to-date critical information lists and must ensure that all employees are trained to protect sensitive information from public release. Commanders shall ensure public affairs officers and Web site managers work closely with OPSEC officers to ensure adequate processes are developed to prevent inadvertent disclosure of information, including sensitive unclassified information, via the public domain.

4. All Army OPSEC officers should update their OPSEC Orientation and Annual Refresher Briefings to include training regarding the vulnerabilities associated with the use of internet and social media sites. OPSEC officers who need assistance with the development of materials to include in Command briefings should contact the Army OPSEC Support Element, 1st IO Command, 703-428-4785 or 703-428-4506. ACOM,

ASCC, and DRU OPSEC Program Managers are required to report the status of updates made to their awareness programs through the annual reporting process, conveyed in AR 530-1, Appendix I.

5. Social networking sites provide opportunities for adversarial groups, such as foreign intelligence services, to glean personal information for use in directly targeting Army and DoD users. All Army personnel have a personal and professional responsibility to ensure no information that might place Soldiers in jeopardy or be of use to adversaries (including local criminal elements) be posted to public Web sites. Sensitive organizational information (to include sensitive, unclassified information) shall not be discussed on any externally facing Web site. The following list includes, but is by no means a comprehensive list of, examples of information that should never be published on a public Web site:

- a. Classified information
- b. Casualty information before the next-of-kin has been formally notified by the Military Service concerned
- c. Information protected by the Privacy Act
- d. Information regarding incidents undergoing investigation
- e. Information considered Essential Elements of Friendly Information (EEFI)
- f. For Official Use Only information
- g. Information identified on the current Critical Information List
- h. Personally Identifiable Information (PII)
- i. Sensitive Acquisition or contractual information

6. To assist in identifying risks associated with implementation of social media sites and to provide advice on secure implementation, each Army organization will contact the appropriate IA Manager and Privacy Act Official. The requirements of the information security program address the safeguarding and disclosure of both classified and sensitive information and both will be afforded the level of protection against unauthorized disclosure, commensurate with the level of classification and sensitivity assigned. All Army personnel are responsible for ensuring that classified and sensitive information and materials are adequately protected from compromise.

7. Official government sites are established on commercial social networking commercial venues for the purposes of creating a transparent information-sharing environment and gaining feedback from the public by exception only. If Web sites, to include social media sites, on the .com domain are being used outside of those exceptions in AR 25-1 (which includes public affairs, education, and recruiting purposes) a waiver is required. Requests for waivers must be submitted by the HQDA element or parent command through Headquarters, Department of the Army CIO/G-6 (SAIS-GKP), 107 Army Pentagon, Washington, DC 20310-0107. Due to exploitation and elicitation exposure and risks, all Army sites or accounts operating in an official capacity will not be used for personal use, must be linked to an Army Knowledge Online (AKO) email address, and must never be used to communicate directly with family, friends, or other official Army or government representatives. Content posted on these sites by the site administrator(s) will not contain political or discriminatory content, and

not endorse or appear to endorse or show favoritism to nonfederal entities. Content or views posted on these sites by the site administrator(s) must reflect U.S. Government policy and may not appear to endorse views contrary to U.S. Government policy.

8. Those with an approved exception to establish and maintain official social media sites on a commercial Web site must: validate the security and management of the systems and networks to be used; annually complete updated OPSEC training as described in paragraph 4 of this document; and ensure Public Affairs, Privacy, and OPSEC reviews of content before release or disclosure. All information contained on publicly accessible Web sites is subject to the policies and clearance procedures described in AR 360-1, chapter 5, for the release of information to the public. Furthermore, all organizations engaging in social media must consider records management requirements as detailed in AR 25-400-2.

9. DoD/DA employees and contractors may establish personal accounts on social media sites. However, personal accounts should not be established with government email addresses, employ the use of government logos, be used to conduct official business, release official agency information, or be used for any other official communication related to the employee's government job or activities. Agency personnel utilizing social media technologies must comply with the Joint Ethics Regulation, and the Standards of Ethical Conduct for Employees of the Executive Branch, (see: Ref A, 5 CFR Part 2635). These rules include the prohibition of release of non-public information, require appropriate disclaimers of opinions being expressed, and restrict the use of government computers to access and manage personal sites during official duty time.

10. The Risk to Army and personal information must be understood by all Soldiers, Civilians, and Family members. Personnel must discuss the proper use of social media technology with their Family members in order to protect them from the inadvertent release of sensitive information.

Glossary of Collaborative Technologies

Aggregator: A site that gathers information from multiple web sites, typically via RSS. Aggregators let web sites remix the information from multiple web sites, for example by republishing all the news related to a particular keyword.

Blogs: A frequently updated, chronologically ordered publication of personal thoughts and opinions with permanent links to other sources, creating a historical archive. This can be published on personal websites or institutional websites as communication tools.

Mashup: A web application that combines data from more than one source into a single integrated tool. For example, the use of cartographic data from Google Maps to add location information to real-estate data from Craigslist, thereby creating a new and distinct web service that was not originally provided by either source.

Open-source software: Software developed in the public domain by multiple developers that is available for sharing, enhancing, and various other uses. Linux and Pearl are good examples.

Peer-2-peer (P2P) Computing: Allows direct sharing of files from one user PC to another user's PC using the web as the platform. Examples of P2P computing include BitTorrent, Gnutella, and FreeNet. Such P2P connections between users can form large networks that can also be used to distribute telephony in real time.

Perpetual beta: A term used to describe software or a system that never leaves the development stage of beta. Perpetual beta has come to be associated with the development and release of a service in which constant updates are the foundation for the habitability/usability of a service, as is common with many Web 2.0 applications.

Podcasts and vlogs: Online audio and video blogs that can be downloaded to devices such as PCs or handheld devices (wireless phones, mp3 players, iPods). These can be subscription based or free, single-use or repeated use content.

Really Simple Syndication (RSS): A family of web-feed formats used to push frequently updated content such as blog entries, news headlines, or podcasts to users' PCs or devices. An RSS document, which is called a "feed," "web feed," or "channel," contains either a summary of content from an associated website or the full text. RSS makes it possible for people to keep up with their favorite websites in an automated manner that's easier than checking them manually.

Social networking sites: Online networking platforms that allow registered users to interact with other users for social or professional purposes. Examples include MySpace, Facebook, and LinkedIn.

Social bookmarking: The collaborative equivalent of storing favorites or bookmarks within a web browser, social bookmarking services (like del.icio.us or Furl) let people store their favorite web sites online. Social bookmarking services also let people share their favorite web sites with other people, making them a great way to discover new sites or colleagues who share your interests.

Tag: a keyword or term associated with or assigned to a piece of information. Often used to classify items such as blog posts, photos, or mapped locations into specific categories or taxonomies.

Virtual worlds: A computer-based simulated environment intended for its users to inhabit and interact via avatars. This habitation usually is represented in the form of two- or three-dimensional graphical representations of humanoids (or other graphical or text-based avatars). Most, but not all, virtual worlds allow for multiple users. The world being computer-simulated typically appears similar to the real world, including features such as gravity, topography, locomotion, real-time actions, and communication.

Communication has, until recently, been in the form of text, but now real-time voice communication using VoIP is available. This type of virtual world is now most common in massively multiplayer online games. Examples include Active Worlds, ViOS, There, Second Life—although not games per se but more like virtual environments that can include gaming—Entropia Universe, The Sims Online, Red Light Center, Kaneva. Particularly massively multiplayer online role-playing games include EverQuest, Ultima Online, Lineage, World of Warcraft, RuneScape, AdventureQuest, and Guild Wars.

Wikis: Collaborative publishing technology that allows multiple users to work on and publish documents online with appropriate version control. Wikis allow hypertext links to content in any form, enhancing user experience and interactions.