



DEPARTMENT OF MILITARY AND VETERANS AFFAIRS
OFFICE OF THE ADJUTANT GENERAL
COMMONWEALTH OF PENNSYLVANIA
FORT INDIANTOWN GAP
ANNVILLE, PENNSYLVANIA 17003-5002
www.dmva.state.pa.us

PAO

6 November 2013

MEMORANDUM FOR Department of Military and Veterans Affairs; Pennsylvania Army and Air National Guard personnel; and all other organizational entities

SUBJECT: Policy for Official PA Guard Social Media as Directed by DoD

1. References:

- a. 5 CFR Part 2635, Standards of Ethical Conduct for Employees of the Executive Branch.
- b. Directive Type Memorandum DTM 09-026, Responsible and Effective Use of Internet Based Capabilities, 25 February 2010.
- c. DoD Directive 5400.11, "DoD Privacy Program," 8 MAY 2007.
- d. DoD Directive 5230.09, Clearance of DoD Information for Public Release, 22 AUG 2008.
- e. DoD Directive 5500.7-R, Joint Ethics Regulation, 29 NOV 2007.
- f. Secretary of the Army Memorandum – Delegation of Authority – Approval of External Official Presences, 21 OCT 2010.
- g. CIO/G6 Memorandum, Use of Social Media Tools, 27 AUG 2009.
- h. CIO/G6 Memorandum, Responsible Use of Internet Based Capabilities, 2010.
- i. Army Regulation 25-1, Army Knowledge Management and Information Technology Management, 4 DEC 2008.
- j. Army Regulation 25-2, Information Assurance, 23 MAR 2009.
- k. Army Regulation 25-400-2, The Army Records Information Management System (ARIMS), 2 OCT 2007.
- l. Army Regulation 360-1, The Army Public Affairs Program, 25 MAY 2011.
- m. Army Regulation 380-5, Department of the Army Information Security Program, 29 SEP 2000.

PAO

SUBJECT: Policy for Social Media as Directed by DoD

- n. Army Regulation 530-1, Operations Security, 19 APR 2007.
- o. Army Social Media Handbook, 12 JUN 2012.
- p. Air Force Instruction 35-101, Public Affairs Mission, 18 AUG 2010.
- q. Air Force Instruction 35-107, Public Web Communications, 21 OCT 2009.
- r. Air Force Instruction 35-113, Command Information, 11 MAR 2010.
- s. Air Force Instruction 33-129, Web Management and Internet Use, 03 FEB 2005.
- t. Air Force Guide to Effective Social Media Use, MAR 2012.
- u. National Guard Bureau Public Affairs Manual 360-5, 6 Jun 2008.
- v. PA Department of Military and Veterans Affairs Policy Information Memorandum 11-009, Information Technology and Social Media Acceptable Use Policy 27 APR 2011.
- w. Commonwealth of Pennsylvania Management Directive 205.34, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy, 17 NOV 2011.

2. Applicability.

a. IAW DoD regulations, the following social media outlets are approved for O6 commands and higher to include JFHQ directors, the 28th Infantry Division Commander, the 213th Regional Support Group Commander, maneuver brigade commanders, TDA units (Med. Det, 166 Regiment, EAATS, and FTIG Training Site), and PaANG wing commanders:

- (1) Facebook
- (2) Flickr
- (3) YouTube
- (4) Twitter

b. The following social media outlets are approved for all PAARNG and PaANG O5 commands:

- (1) Facebook
- (2) Twitter

PAO

SUBJECT: Policy for Social Media as Directed by DoD

c. Official social media presences below the O5 command level are not authorized at this time. Unit leaders at the company level or below who wish to have a social media presence may request administrative privileges from the next highest entity in their chain of command and, if approved, post materials to those pages.

3. Policy.

a. In order to aid with unit cohesion, broaden the range of command information, and assist with recruiting, PAARNG and PaANG O5 commanders (and higher) are encouraged (but not required) to establish and use the social media sites approved at their levels.

b. Since both civilian and military publics have access to information that appears on social media sites, a commander should choose to establish an official presence only if he/she has determined the benefits of establishing such a presence outweigh any risk to operational security (OPSEC).

c. Commanders who choose to initiate an online presence must assign a minimum of two (one of whom must be full-time) National Guard Knowledge Managers, who will be given administrative privileges to post information to the sites while frequently monitoring the site for misuse.

d. All sites will be requested through each public affairs office in the requesting unit's normal military chain of command, with final approval/disapproval by the State Public Affairs Office. The State PAO will aid with format and ensure sites comply with standards established by the Department of Defense.

e. As an added security measure, a minimum of one full-time knowledge manager from each higher level of the hosting unit's chain of command and no fewer than two members of the full time State PAO staff will be given administrative rights to all PNG sites, which will be used to add, delete, or alter content as necessary to maintain command policies and standards. Units will be notified when content that has been deemed inappropriate has been removed.

f. Commanders are responsible for content posted on their pages and must ensure that comments posted to his/her site are immediately removed if not in compliance with posting guidelines outlined in this memorandum.

5. Posting Guidelines.

a. Content. Pursuant to TAG-PA guidance, noncompliance with the following guidelines will result in removal of messages by the site administrator(s) and could result in disciplinary action for military members:

(1) Graphic, obscene, explicit or racial comments or submissions and comments that are abusive, hateful or intended to defame anyone or any organization.

PAO

SUBJECT: Policy for Social Media as Directed by DoD

(2) Solicitations or advertisements. This includes promotion or endorsement of any financial, commercial, or non-governmental agency. Similarly, there will be no allowance of attempts to defame or defraud any financial, commercial, or non-governmental agency.

(3) Comments suggesting or encouraging illegal activity.

(4) Copyrighted or trademarked material including embedded music or links to un-attributed artwork.

(5) Derogatory comments expressed against the chain of command. This includes both members of the military and civilians assigned or elected to government positions.

(6) Comments considered inappropriate, unprofessional, or unbecoming to a Soldier's/Airman's position within the PA National Guard.

(7) Individuals using rank, job, and/or responsibilities in order to promote him/herself for personal or financial gain.

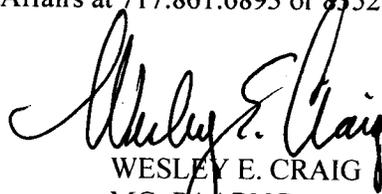
b. Operations Security. All OPSEC guidance will be observed and content will be limited to only PAO approved releasable material(s). Releasable content may be (but not limited to) text, digital photographs, digital video, and digital audio.

(1) When posting to any social media site, administrators will avoid mentioning OCONUS unit locations, troop movement dates/times, or equipment specifications/ capabilities. Comments to posts by others to the site that mention the above subjects will be removed immediately.

(2) Photos that include geographical location data (also known as "geotagging") will not be posted to sites.

(3) Do not post information regarding times and dates of future formations that could be used to coordinate attacks on military members. This includes drill schedules, training schedules and dates of upcoming exercises and deployments.

6. Point of Contact. All questions regarding official social media sites should be directed to the Pennsylvania National Guard Office of Public Affairs at 717.861.6893 or 8352.


WESLEY E. CRAIG
MG, PAARNG
The Adjutant General