**DEPARTMENT OF THE ARMY**
**HEADQUARTERS UNITED STATES ARMY MANEUVER CENTER OF EXCELLENCE**
**1 KARKER STREET**
**FORT BENNING GEORGIA 31905-5000**

REPLY TO
ATTENTION OF

Policy Memorandum 360-1-4

ATZB-PO

24 JAN 2019

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Maneuver Center of Excellence Internet-Based Capabilities and Social Media Policy

1. REFERENCES:

a. DoD Instruction 8170.01 (Online Information Management and Electronic Messaging, December 31, 2018.

b. DoD Directive 5230.9 (Clearance of DoD Information for Public Release), August 22, 2008, Certified Current through Aug 22, 2015, Incorporating Change 2, Effective April 14, 2017.

c. DoD Directive 5400.11 (DoD Privacy Program), October 29, 2014.

d. DoD Directive 5400.11-R (DoD Privacy Program), May 14, 2007.

e. DoD Directive 5205.02E (DoD Operations Security (OPSEC) Program), June 20, 2012.

f. Memorandum, SECDEF (A&M), 9 November 2001, subject: Withholding of Personally Identifying Information under the Freedom of Information Act.

g. Memorandum, Assistant SECDEF (C31), 28 December 2001, subject: Removal of Personally Identifying Information for DoD Personnel from Unclassified Websites.

h. Memorandum, Secretary of the Army, 2 December 2013, subject: Delegation of Authority, Approval of External Official Presences.

i. Office of the Chief of Public Affairs Memorandum, Standardizing official U.S. Army external official presences (social media), 10 January 2014.

j. AR 25-1 (Information Management Army Information Technology), 25 June 2013.

k. AR 360-1 (The Army Public Affairs Program), 25 May2011.

l. AR 380-5 (Department of the Army Information Security Program), 29 September 2000.

m. AR 530-1 (Operations Security (OPSEC)), 26 September 2014.

n. TRADOC Reg 25-1 (Information Resources Management), 16 September 2006, Change 1, 16 April 2008.

o. TRADOC Reg 350-6 (Enlisted Initial Entry Training Policies and Administration), 20 March 2017, Change 1, 30 January 2018.

p. The United States Army Social Media Handbook: https://www.army.mil/socialmedia

q. Hatch Act Guidance on Social Media: https://osc.gov/Resources/HA%20Social%20Media%20FINAL%20r.pdf

2. PURPOSE: To establish requirements and guiding principles for the implementation and effective use of official U.S. Army social media sites (also known as External Official Presences, or EOPs) and public-facing .mil websites by the Maneuver Center of Excellence and Fort Benning organizations, and set standards of conduct for participation by personnel on official sites. Partner organizations are invited to participate in this policy. Sharing of administrative/posting rights enhances integration of communications and overcoming continuity issues when staffs are short.

3. APPLICABILITY: This policy applies to all MCoE and Fort Benning information residing on the publicly-accessible web.

4. POLICY: The guidelines set forth in this document reinforce and build on the Army Social Media Handbook and help to ensure the official use of social media presences by MCoE and Installation Management Command (IMCOM) organizations is necessary and effective.

a. External official presences (EOPs) not located on the .mil domain:

(1) Leaders will appoint a representative as a social media manager (SMM) with the responsibility of maintaining the organization's official presence(s) on all Internet-Based Capabilities. This individual should become familiar with Army Social Media and Web Policies including the Army Social Media Handbook. The MCoE Web Content Manager (WCM) will provide Social Media resources as needed.

(2) See Enclosure 1 for Checklist for Establishing an Official MCoE or Fort Benning Social Media Presence.

(3) The MCoE and Fort Benning units are expected to maintain the following web presences in order to contribute to the MCoE 4th Line of Effort—Community Relations:

(a) Due to their unique community outreach mission, basic training units are required to maintain an official Facebook page for each company in the unit.

An SMM for each company will be designated to update and monitor each company page. Mandatory updates include:

- Welcome letter.
- Graduation information.
- Three to five photos per week with photo description in line with OPSEC regulations.

(b) All other units must maintain an official Facebook page at the brigade or directorate level.

An SMM for each brigade or directorate will be designated to update and monitor each company page. Mandatory updates include one photo per week with photo description in line with OPSEC regulations.

(c) Additional guidance for all unit EOPs is as follows:

(1) The "About" tab on all EOPs must be updated with current information. Mandatory information is as follows:

- Address: Physical location of unit headquarters building.

- Phone number: Staff duty phone number.

- E-mail: Use a generic e-mail account that multiple users can access.

- Website: Unit's official .mil website.

(2) All SMMs and alternate SMMs must take two online trainings:

- https://iatraining.us.army.mil

- https://iase.disa.mil/eta/sns_v1/sn/launchPage.htm

(3) Release authority for all information on the unit EOP resides with the SMM. The SMM will screen information against the unit Critical Information List and avoid posting information that would violate OPSEC regulations.

(4) Unit EOPs are not a place for personal or commercial advertisements, or endorsements. Such activity implies U.S. Army endorsement and should be avoided except by authorized MWR Marketing and AAFES EOPs.

b. Personal Websites, social media, and other Internet-based capabilities.

(1) Personal Internet Home pages, message boards, blogs, web-based video logs, standard e-mail, wireless devices, and other evolving forms of electronic media have become increasingly popular as convenient means for Army personnel to communicate in real and near-real time with Families, friends and the general public (national and international). The increased speed and capability of digitized and wireless communications requires increased personal and unit responsibility. Soldiers and Civilians, regardless of rank or duty position, are required to protect information in order to prevent the nation's adversaries from acquiring and using that information against the United States.

(2) Soldiers using social media must abide by the Uniform Code of Military Conduct (UCMJ) at all times. Commenting, posting or linking to material that violates the UCMJ is prohibited. Social media provides the opportunity for Soldiers to speak freely about their activities and interests. However, Soldiers are subject to UCMJ even when off duty, so talking negatively about supervisors or releasing sensitive information may be punishable under the UCMJ. It is important all Soldiers know that once they log on to a social media platform, they still represent the Army.

(3) Leaders must hold personnel accountable for adherence to OPSEC regulations and any other applicable policies addressing communication. All Government employees understand that they are responsible for the content of their Internet-Based Capabilities (IBC).

(4) Personal websites and blogs produced in a personal capacity and not in connection or reference to official duties require no advance clearance.

(5) Unofficial and personal Websites—in which individuals identify themselves as Soldiers or Civilians affiliated with the U.S. Army—must comply with all DOD and local command policies.

(a) It is the personal responsibility of Soldiers, DA Civilians, and DOD contractors to ensure that any personal Websites and blogs do not contain non-releasable information.

(b) Personnel must add a disclaimer to unofficial personal Websites—in which the individual refers to him or herself as a Soldier, employee, or contractor of the U.S. Army—to preclude readers from assuming unofficial sites represent an Army position.

(c) Reasonable restrictions on free speech (such as no political commentary while in uniform) extend to electronic communications.

(d) Questions concerning the sensitivity of information should be submitted for OSPEC and Public Affairs review prior to releasing or posting.

(6) All visual information (still and video imagery) produced in a personal capacity and provided directly to any media outlet, organization, public website, Family, or friends, whether in hard copy or electronic form, is subject to this regulation.

(a) Do not release imagery, digital, still, or video of deceased, wounded, hospitalized, or detained personnel.

(b) Do not release images of battle-damaged vehicles or equipment damaged by improvised explosive devices, direct enemy contact, or any other damages caused by enemy action.

(7) Information placed on or sent over DOD computer systems is subject to monitoring, inspection, and audit by AR 360-1 command or agency management or their representatives at any time with or without notice or user consent. This includes personal information, e-mail, personal user files and directories, and any products created on DOD computer systems. Commanders are encouraged to implement additional guidance or restrictions based on current technologies, areas of operation, atmospherics, or mission parameters.

c. Information publishing guidance is as follows:

(1) Personnel should always assume that the entire world—adversaries, friendly, and neutrals alike—is viewing all transmitted or posted material (e-mail, blog, or personal web page). Government employees are required to review all information and posting to ensure that the information posted will not put themselves, other employees, or their Families at risk.

(2) The Army is a values-based organization. Army personnel will ensure all writings and posting of information appropriately represent or convey the Army Values.

(3) Military personnel and federal employees are prohibited from using their official authority or influence to affect the outcome of an election. This policy extends to official and personal social media and other online presences.

(4) Official, unofficial and personal online presences will not have any information that is considered non-releasable. Non-releasable information is any official information that is generally not available to the public and that would not be released under the Freedom of Information Act. Examples of information prohibited from public release include, but are not limited to, the following:

(a) Classified information.

(b) Casualty information before verification that the next of kin has been formally notified by the military Service concerned.

(c) Information protected by the Privacy Act (for example, age, date of birth, home address, marital status, and race).

(d) Information regarding incidents under ongoing investigation.

(e) Information or imagery of U.S. Coalition Forces without an official release signed by the individuals in advance or of enemy personnel killed, wounded in action, or hospitalized.

(f) Information that misrepresents the Army and statements in conflict with good order, morale, discipline and mission accomplishment.

(g) Photographs containing sensitive images, especially those showing the results of improvised explosive devices strikes, battle scenes, casualties and destroyed or damaged equipment.

5. SUPERSESSION: This policy memorandum supersedes MCoE Policy Memorandum 360-1-14, 17 March 2017, same subject.

6. PROPONENT: The MCoE Chief of Public Affairs at 706-545-9229.

FOR THE COMMANDER:

DOUGLAS G. VINCENT
COL, IN
Chief of Staff

3 Encls
1. as
2. Requesting a Verification Badge for Your Official Facebook Page
3. Official Fort Benning and MCoE Facebook Best Practices

DISTRIBUTION:
ADMIN L, MCoE BN CDRS, MCoE CSM/SGM, and MCoE DCO/XO Lists

## Checklist for Establishing an Official MCoE or Fort Benning Social Media Presence

**Commanding officer or public affairs officer approval.** A presence must be approved by the release authority before it can be registered.

**Study Army social media policy and read Army resources.** Before you get started with social media, it is important to understand Army social media policy. Army social media resources can be found at: www.slideshare.net/USArmySocialMedia.

**Determine your goals and audience.** What do you want to achieve/communicate? It could include distributing command information, connecting to a community, building spirit de corps, etc. Identify the audience you intend to communicate with. This can include Soldiers, Families, Veterans, Army Civilians and the general public. Don't forget, your audience will also include stakeholders, politicians, community leaders and adversaries or enemies.

**Research and select social media platforms.** Identify the social media platforms that will best suit the needs of your organization. Not all platforms will work for some organizations, so make sure you understand what can be achieved with each platform.

**Social media sites must provide links to official MCoE Websites.** This includes the MCoE Website, http://www.benning.army.mil, and the organization's official .mil website (if applicable).

**The presence must post disclaimer text and MCoE user policy.** The disclaimer identifies the page as an "official" Army social media presence and disclaims any endorsement. The MCoE WCM will provide you with the disclaimer and use policy.

**The presence must be clearly identified as "official" and share MCoE and Fort Benning branding.** Site must identify that the presence is "official" somewhere on the page. The MCoE WCM will support you with creating official brands and images, if needed.

**The presence must be unlocked and open to the public.** All official presences are open to the public. Facebook pages must allow users to post onto the wall, and allow users to send private messages.

**Social media presences must be registered and labeled as a Government Organization.** The use of Facebook Profile, Community and Group pages for official purposes violates the government's terms of service agreement with Facebook.

**Set default view of your Facebook wall to show posts by only your organization.**

**Submit the social media presence for approval and registration to www.army.mil/socialmedia.** This applies only to brigade-level units and above.

## Requesting a Verification Badge for your Official Facebook Page

Units under MCoE or Fort Benning should request a gray verification badge (gray check mark) to increase credibility and trustworthiness among our audiences.

**Check eligibility requirements for verification.** Facebook requires you to be an admin of your Page, your Page must be published with profile and cover photos, and have posts.

**Increase your Page credibility before asking for verification.** The following steps will increase your chances of receiving the badge:

- Give your Page a name, preferably the name of your unit. Make sure the name will be found on search engines when people want to find your unit. For example, the MCoE Official Facebook page is @FortBenningMCoE.
- Make your Page recognizable to Facebook by posting professional, on-brand content. You may need to be actively posting for several weeks before requesting a badge.
- Make sure your "About" information is filled in and up-to-date. Use a general inbox, the physical location of your unit HQ, and a staff duty phone number for contact information.
- Make sure your Facebook page is listed on your .mil website. Send a request to the MCoE WCM to get it listed.

**Request the verification badge on Facebook.** Follow these steps to complete the request online:

- Click "Settings" at the top of your Page.
- Click "Page Verification."
- Click "Verify this Page."
- Enter a publicly listed phone number for your business, your country, and your language.
- Click "Call Me Now" to allow Facebook to call you with a verification code.
- Enter the 4-digit verification code and click "Continue."
- If you don't want Facebook to call you, you may choose "Verify this Page with documents instead" at the bottom left of the window that appears. You must upload a picture of an official document showing your business's name and address, such as a utility or cable bill.

Encl 2

## Official MCoE and Fort Benning Facebook Best Practices

**Online conduct.** You are responsible for all content you post to your social media platforms, both official and unofficial. Maintain your professionalism at all times.

**Pinned posts.** Social media managers can pin one post at the top of the page to make it easily viewable. For example, training companies can pin their Welcome Letter to the top of the page at the start of each cycle.

**Photo content.** Do not post photos to check the block. Photos should convey a message and tell your organization's story. Be aware of backgrounds and foregrounds—always be on the lookout for OPSEC!

**Captions and text updates.** Write for your audience! Avoid military jargon and acronyms, and really spell out what the photo is depicting with descriptions civilians can understand.

**Message auto-responses.** Use an auto-response for your Facebook messenger. Thank users for their message, tell when they can expect a response back by, and link to your official .mil for more immediate information. Auto-responses can be up to 255 characters.

**Comment filters.** You can block certain words from appearing in comments on their Pages. The process for blocking words is as follows:

- Click "Settings" at the top of your Page.
- Click "Page Moderation" in the "General" Tab.
- Type the words you want to block, separated by commas. Note: you will need to add all forms of the word (verb tenses, plural/singular, etc.)
- Click "Save Changes."

Facebook also has a profanity filter already built into their Page controls. Ensure your Page's profanity filter is set to strong.

**Responding to comments.** Talk with your audience, not at them. If users ask a question in the comments, feel free to respond candidly. If the question and response involve negative feedback or private information, invite the user to send you a private message.