



PAMBANSANG PUNONGHIMPILAN TANODBAYBAYIN NG PILIPINAS
(National Headquarters Philippine Coast Guard)
139 25th Street, Port Area,
1018 Manila

26 March 2020

NHQ-PCG / CG-2

CIRCULAR
NUMBER 03-20

PHILIPPINE COAST GUARD ONLINE PRESENCE AND USE OF SOCIAL MEDIA

I. REFERENCES:

- a. PCG Regulations G 200-001, Security of Classified Matters dated 23 Sept 2002
- b. HPCG Circular Nr 09-14 dated 01 September 2014, Policy Guidelines to Raise Security, Awareness, Consciousness, and Discipline on the Use of Information and Communications Technology (ICT) Devices and the Internet of PCG Personnel;
- c. HPCG/CGIAS Circular Nr 06-16 dated 30 August 2016, Guidelines and Procedures on Disposition of Violations of Code of Conduct and Discipline for PCG Uniformed Personnel;
- d. Republic Act 10175, Cybercrime Prevention Act of 2012
- e. Republic Act 9995, Anti-Photo and Video Voyeurism Act
- f. Omnibus Rules Implementing Book V of Executive Order Nr 292 and other pertinent Civil Service Laws
- g. OTAG/PCRD Letter Directive Nr 15 dated 13 March 2013
- h. HPA Directive on the Use of Social Media dated 05 Sept 2013
- i. U.S Coast Guard Social Media Handbook V.2015

II. PURPOSE:

The purpose of these guidelines is to lay out the Command's policies to be strictly followed by all personnel working in the PCG organization, uniformed and civilian alike, in establishing and maintaining an online presence in enabling PCG personnel and civilian employees to make full use of personal online presence while protecting their own and the PCG's interest. It sets the guidelines on the conduct of all PCG units and offices on the usage of social media.

III. DEFINITION OF TERMS:

For the purpose of this guideline, the following words and phrases shall be defined as:

A. **Social Media** – a form of electronic communication through which users create online audiences and communities to share information, ideas, personal messages, and other content. It is a highly interactive tool for reaching large audiences.

B. **Website** – a collection of web pages that are accessed through the internet when a web address is typed, clicked on a link, or put as a query in a search engine. It can contain any type of information, and can include text, color, graphics, animation and sound.

C. **Electronic Mail (Email)** – a method or system of exchanging messages electronically from an author to one or more recipients (as between computers on a network).

D. **Internet** – an electronic communications network that connects computer networks and organizational computer facilities around the world.

E. **Indecent** – offending or grossly impolite terms of words, deeds and views against generally accepted standards of propriety or good taste.

F. **Classified Information** – in any form or of any nature, the safeguarding of which is necessary in the interest of national security and which is classified such purpose by the responsible classifying authority. It includes all information concerning documents, cryptographic devices, development project and materials, falling in the categories of top secret, secret, confidential or restricted.

G. **Posts** – information in the form of words, documents, pictures, sounds, and videos that are published, announced, or advertised publicly or privately in the internet.

H. **User** – an individual who interacts and publicizes information, comments, opinions and suggestions on social media.

I. **Blog** – (a contraction of the term “web log”) is a type of website that contains an online journal or diary with reflections, comments, and often hyperlinks provided by the writer.

J. **Hyperlinks** – are references to data that the reader can directly follow, or that is followed automatically. A hyperlink points a whole document or to a specific element within a document.

K. **Netiquette** – (short for “network etiquette” or “internet etiquette”) is a set of social conventions that facilitate interaction over networks, ranging from Usenet and mailing list to blogs, forums and other online activities.

L. **Online Presence** – any channel or any online means by which an individual or group self-publishes information through the internet, for example a website, blog, photo or video channel, bulletin board account, social network profile, and wiki.

M. **Tagging** – the practice of creating and managing labels (or “tags”) that categorize content using simple keywords. Tags are also special kind of links. For example, an individual can tag a photo to show who’s in the photo or post a status update and say where (geo-tagging) or who the person is with.

N. **Upload** – to transfer data or files from a local system such as a computer, camera or smart phones to a remote system such as a server or a client with the intent that the remote system should store a copy of the data being transferred.

O. **Social Network Administrator** – refers to the PCG Officer/Non-Officer responsible in the filtering of “followers” or “fans”; uploading and tagging of photographs and linkages; providing social media reports concerning maritime related incidents; and updating and commenting on information involving issues concerning the PCG. It is also referred to as Focal Person in unit/office where there is no assigned PIO designated to perform the above responsibilities.

IV. POLICIES AND PROCEDURE:

A. As a matter of general policy, social networking sites, blog and wiki sites and photo and video sharing sites are not allowed to run within the PCG networks. As such, respective network administrators shall block said sites.

B. While the PCG realizes and recognizes the fact that there are also units and offices within the PCG that need to run, monitor, put up or maintain said sites or engage in online activities for official purposes that are in line with or in support of the mission and functions of the unit or offices, these said units or offices shall conduct these authorized online activities outside of the PCG networks through their own internet service providers.

This guideline, therefore, shall allow PCG units and offices to operate and maintain said online activities, provided that the computers, portable devices, mobile devices or other similar electronic devices that will be used for such online activities shall have their own internet service provider and shall not connect to the respective PCG networks.

C. The Spokesperson shall be the official source of “public information” for and on behalf of the PCG Organization. On the same manner, there shall also be a designated Social Network Administrator in every PCG unit/office that will ensure proper utilization of the Official PCG Social Networking Accounts.

D. Official PCG Social Networking Accounts

1. Only official PCG e-mail addresses shall be used when creating all official PCG social networking accounts.

2. For existing accounts, the designated social networking administrator must check whether or not these were created with the official PCG e-mail.

3. If items (1) and (2) are not observed, the social media accounts shall be deemed "unofficial" and shall be deleted.

4. The following naming convention, to the extent possible, shall be used by all PCG units and offices in naming their social networking accounts:

a. PCG commands, districts, units, and offices shall spell out their entire name; and

b. If there are limits on the number of characters that may be used, the official acronym shall be used.

5. Whenever possible, official PCG social networking accounts must include the following information either in a prominent page or as a link to their official website:

a. Mission and function;

b. Description of the unit office;

c. Citizen's Charter;

d. Contact details, including address, telephone number/s, e-mail, and official website URL; and

e. Participation and Moderation Rules

6. PCG units and offices should be guided by the provisions of relevant laws and issuances when publishing information.

7. Posting or uploading of content shall only be done by authorized personnel, including the designated social network administrator, unit commander or head of office.

8. Contents classified as TOP SECRET, SECRET, CONFIDENTIAL, or RESTRICTED, in accordance with PCG Regulations G 200-001, Security of Classified Matters dated 23 Sept 2002 shall not be posted and the disclosure and/or misuse of such information as stated above is strictly prohibited.

9. The following content is considered blacklisted and shall not be posted in an official PCG networking accounts:

a. Blackmail/insulting content – content which threatens an agency or entity with possible problems in exchange for money, other things of value, or personal advantage;

b. Pornographic content – content which contains lewd, indecent, or sexually connotative words, photographs, advertisement, and the like;

c. Malicious content – content which shows an intention to discredit an entity/office or a government representative without basis or substantial proof or evidence;

d. Unauthorized posting of copyrighted material – content that is copyrighted-protected material such as books, publications, or research that is posted without the permission of the author/issuing organization, except as may be allowed under RA 8293, as amended by RA 10372, otherwise known as the intellectual property code of the Philippines;

e. Unrelated information, jokes, or promotions – content containing unrelated or irrelevant advertisements, links, personal jokes, social media pages, and other information not of value to the PCG;

f. Suspicious links and viruses – content with links to files or websites which may post security threats to PCG; and

g. Opinion – content made by PCG personnel or civilian employees, which do not represent the PCG's or unit/offices' view.

10. PCG personnel and civilian employees shall not publish photos, videos and other information regarding future, present or past PCG operations or activities online. However, PCG activities, official statements, press release, and other publications that are for public consumption are allowed content.

E. Personal Social Networking Accounts

1. The PCG also realizes and recognizes that uniformed and civilian personnel have some privileges and right to self-expression and may engage in such online activities mentioned above, provided:

a. That the information or any output that shall emanate from said online activities shall not harm other persons; shall not put other people in an embarrassing, inconvenient or humiliating position; and shall not be detrimental to his/her unit, in particular, or the PCG, in general, and its respective interest and security;

b. That the person or group shall be aware and guard against security risks that are involved and as an offshoot of the online activity;

c. That permission should be sought from their respective Unit Commanders or Chief of offices, through the advice of their respective Social Network Administrator in publishing any information which will reflect his/her Unit's activities;

d. That proper netiquette and a high standard of conduct and behavior online shall be adhered to and that proper respect on the privacy and security of others is observed;

e. That the information or data that shall be posted shall not be misconstrued as an official release or statement of the Department of Transportation or the entire PCG organization. Personnel who seek to publish any information relating to the PCG shall use a disclaimer that such publication is undertaken in his personal position/opinion and does not necessarily represent the official statement of the PCG; and

f. That any post, tags, online comments, videos, photo and all other media uploads; and any other forms of online activity shall not violate existing laws, policies, and regulations.

2. PCG personnel and civilian employees shall take utmost precaution in identifying themselves online as uniformed personnel or as civilian employee working for the PCG since there may be serious personal, privacy, and security risks. Moreover, they must be vigilant of the dangers in sharing information online such as personal information and account details which may be used by some nefarious personalities or criminals to target, stalk, harass or for their illegal purposes.

3. PCG personnel and civilian employees shall not publish photos, videos and other information regarding future, present or past PCG operations or activities online. Said actions may be detrimental to future and present PCG operations. Meanwhile, there are other official means in officially publishing past PCG unit or group activities, as authorized, such as the units' respective websites, which shall act as the units' show window to the online community. Likewise, the following content is considered blacklisted and shall not be posted:

- a. Blackmailing/insulting content – which threatens an agency or entity with possible problems in exchange for money, other things of value, or personal advantage;
- b. Pornographic content – content which contains lewd, indecent, or sexually connotative words, photographs, advertisements, and the like;
- c. Malicious content – content which show an intention to discredit an entity/office or a government representative without basis or substantial proof or evidence.

4. Information and other data posted or published online, such as photo tags, etc., involving other people/personnel such as Unit Commanders, Chiefs of Offices, senior officers, junior officers, subordinates, peers and other personnel shall not be allowed unless there is an explicit permission from the concerned individual.

5. Grievances against the government, other personal issue against fellow government employee, and political comments shall not be allowed to be posted

online. All PCG personnel and civilian employees must express the same in proper organization procedures.

6. All PCG personnel and civilian employees must be vigilant in protecting personal privacy and privacy of others online, it should be observed by preventing internet-related crimes, like identity theft on social media sites by maintaining privacy settings.

7. Posting and disclosing internal PCG documents, information, and operations that the PCG has not officially released to the public are strictly prohibited.

8. All PCG personnel and civilian employees shall be held responsible and liable for unauthorized post, tags and other unauthorized online activities mentioned in this policy that were made by their respective dependents.

9. PCG personnel and civilian employees can act anonymously or pseudonymously in a personal capacity but must:

- a. follow this policy;
- b. be aware that very few things on the internet are genuinely anonymous and most can be traced; and
- c. the PCG and other authorities will penalize serious breaches of the rules, regardless of the intention to punish anonymously.

F. The Unit Commanders and Chief of Offices shall have overall responsibility for the strict implementation of this policy including its proper dissemination and constantly reminding respective personnel of the provisions of this policy and overseeing that resources are also utilized accordingly. Unit Commanders and Chief of Offices may also formulate additional and specific policies, programs and procedures to complement this SOP as deemed necessary. He shall ensure that all violations thereof shall be promptly reported, investigated, and appropriate corrective measures and sanctions shall be imposed. Likewise, respective unit commanders and chief of offices may be held liable and responsible for non-compliance of the provisions of this policy within the organization or office.

G. CGIF shall be responsible for monitoring PCG personnel and civilian employees who violate provisions of this policy. Further, they shall also be responsible for reporting said individuals so that proper charges shall be brought up against said individuals.

H. CGWCEISS shall be responsible in making sure that unauthorized online activities mentioned in this policy are blocked from the PCG networks.

VI. PENAL CLAUSE:

Any violation of this policy will result to disciplinary action under pertinent PCG Regulations G 200-001, Security of Classified Matters and HPCG/CGIAS Circular Nr

06-16, Guidelines and Procedures on Disposition of Violations of Code of Conduct and Discipline for PCG Uniformed Personnel.

VII. REPEALING CLAUSE:

Any issuances, memoranda, rules, and regulations issued by the PCG inconsistent herewith are deemed repealed or amended accordingly.


VIII. EFFECTIVITY:

This Circular shall take effect fifteen (15) days after its publication by the Coast Guard Adjutant.

BY COMMAND OF ADM GARCIA:

OFFICIAL:

JOSE WILLIAM U ISAGA
RADM **PCG**
Chief of Coast Guard Staff


MA IVY C BOTICARIO
ENS **PCG**

Acting Coast Guard Adjutant