U.S. Marine Corps

2021 SOCIAL MEDIA HANDBOOK

TABLE OF CONTENTS

INTRODUCTION

This handbook will familiarize you with policies, guidance, and recommendations on how you can become a more effective communicator and representative of the Marine Corps — creating an environment where trusted information is shared with our Marine Corps family and the public.

Social media, when used effectively, presents unequaled opportunities to share our Marine Corps story in an authentic, transparent, and rapid manner — while building more substantive relationships with people you may not have reached through traditional communication channels.

At the same time, the open, global nature of social media creates challenges and presents operational and cybersecurity considerations and concerns regarding online conduct, including cyberbullying, harassment, and privacy concerns. Careful decisions on the best platforms to use will ensure you convey the relevant information via the most effective means as platforms rapidly adapt, age-out, or emerge.

Social media is only one part of a command's public affairs program. Marine leaders need to work with their Communication Strategy and Operations (COMMSTRAT) team to decide whether social media is appropriate for their command; not every command needs to use social media. If you decide social media would benefit your command, evaluate each platform to determine where your efforts will have the most impact; you don't need to use every platform. Additionally, if you can't maintain your official web presence, it's best not to attempt to manage a social media account

"WE MUST COMMUNICATE WITH PRECISION AND CONSISTENCY, BASED ON A COMMON FOCUS AND A UNIFIED MESSAGE."

Gen. David H. Berger, Commandant of the Marine Corps

COMMUNICATION STRATEGY AND OPERATIONS

COMMSTRAT professionals are responsible for providing timely and accurate information so that the public, Congress and the news media may assess and understand the facts about national security, defense strategy, and the Armed Forces of the United States. Their duty to inform also involves ensuring the free flow of general and military information, without censorship or propaganda, to the men and women of the Armed Forces.

Marine Corps COMMSTRAT professionals work closely with senior leaders and unit commanders to deliver credible and relevant information to these broad audiences through a variety of means. In doing so, COMMSTRAT personnel help educate and inform the public on the mission of the Marine Corps, its role in national defense, and current matters affecting Marines, Sailors, and their families.

Social media is an important tool that, when used effectively, enables individuals and organizations to quickly share information, build and engage online communities, and receive and assess feedback. Marine Corps COMMSTRAT personnel are active on a variety of social media platforms and are responsible for training and educating Marines on the proper use and techniques for online engagement.

The Communication Directorate recommends that commanders without a COMMSTRAT section appoint a Unit Information Officer (UIO) to serve as the direct link to the COMMSTRAT section of the parent command. Through this relationship, COMMSTRAT helps UIOs manage the content on the unit website, advise on social media engagement, and attract coverage to newsworthy events involving the unit and its personnel.

Facilitating the free flow of information while preserving security, respecting privacy, and maintaining proper conduct are critical considerations for all social media users. While COMMSTRAT personnel and UIOs can help prevent unauthorized disclosure of sensitive information, it is the individual responsibility of each social media user to ensure information disclosed or shared online does not jeopardize operational security, threaten the safety or privacy of U.S. Government personnel or their families, or violate applicable policy or law.

GUIDANCE FOR COMMAND SOCIAL MEDIA

All official accounts must be public, and also identified as a government organization, if the platform allows that identification. These accounts are considered official because they are created and managed using federal government resources (including time, manpower, and funds). Social media managers shall be authorized by their commanders to release official information on behalf of their unit and organization.

OFFICIAL USE OF SOCIAL MEDIA FOR MARINE CORPS COMMANDS

Marine Corps social media sites are official representations of the Department of the Navy (DoN) and must demonstrate professionalism at all times. While third-party sites such as Facebook and Twitter are not owned by the DoN, there are guidelines for the management of Marine Corps social media accounts.

POLICY

Department of Defense Instruction (DoDI) 8550.01, released Sept. 11, 2012, discusses the use of Internet-based capabilities (IbCs), such as social media, and provides guidelines for their use. The instruction acknowledges IbCs are integral to operations across the Department of Defense (DoD). It also requires the NIPRNet be configured to provide access to IbCs across all DoD components while balancing benefits and vulnerabilities. By definition, IbCs don't include command or activity websites.

DoDI 8550.01 requires that all official social media presences be registered. Official Marine Corps social media sites need to be registered at *https://www.marines.mil/News/Social-Media*.

SECNAVINST 5720.44C Change 1, Department of the Navy Public Affairs Policy & Regulations, provides policy for the official and unofficial (personal) use of social media, and for the content and administration of official Marine Corps presences on social media, to include:

ADMINISTRATORS:

Commands shall designate administrators for official use of IbCs in writing. The administrator is responsible for ensuring postings to the IbCs comply with content policy. Commands permitting postings by others must ensure the site contains an approved user agreement delineating the types of information unacceptable for posting to the site and must remove such unacceptable content. At a minimum, the DoN's current social media user agreement is required, available at *https://www.marines.mil/News/Social-Media/*.

LOCAL PROCEDURES:

Commands must develop written local procedures for the approval and release of all information posted on command official use of IbCs.

SECURITY:

Commands will actively monitor and evaluate official use of IbCs for compliance with security requirements and for fraudulent or unacceptable use.

PRIMARY WEB PRESENCE:

A command or activity IbC presence may not serve as the DoN entity's primary web presence, and must link to the primary web presence - the command official website. (This means, if your unit does not have its own official website, it cannot have its own official social media.)

PROHIBITED CONTENT:

Commands and activities shall not publish and shall prohibit content such as:

- Personal attacks; vulgar, hateful, violent or racist language; slurs, stereotyping, hate speech, and other forms of discrimination based on any race, color, religion, national origin, disability, or sexual orientation.
- Information that may engender threats to the security of Navy and Marine Corps operations or assets or to the safety of DoN personnel and their families.

CORRECTIONS TO PREVIOUS POSTS:

If correcting a previous post by another contributor on an IbC presence, such posting is done in a respectful, clear and concise manner. Personal attacks are prohibited.

ONLINE ADVERTISING:

With very few exceptions, official accounts may not pay to boost, promote tweets, or take similar action on content — whether on social media platforms, websites, apps or any similar venues. According to the Federal Acquisition Regulation, advertising is defined as "the use of media to promote the sale of products or services." Consult your command's staff judge advocate and/or contracting officer for exceptions and additional information.

DECIDING IF SOCIAL MEDIA IS RIGHT FOR YOUR COMMAND

Communication is commanders' business; commanders are responsible for communicating to Marines and their families. Social media is not a magic wand for all your communication needs. Not every command needs a social media presence. It is far better not to start a social media site than to use it ineffectively and abandon the site. Additionally, if you can't maintain your official website, it's not recommended you to attempt to manage a social media account.

Before launching a social media presence, consider what you want to accomplish. What are your communication objectives and how do they move your command closer to achieving its mission? Is the level of transparency required in social media appropriate for your command and its mission? You also should consider your command's priority publics

and use the right social media platform to reach them. Do you want to communicate with your Marines, Sailors, Marine civilians, command leadership, family members, the local community, a broader DoD audience, or another group altogether? Do you have the content and personnel — both now and long term — to routinely engage with those publics?

Additionally, if your command already has a social media presence, you should routinely ask yourself the above questions to ensure it remains an effective communication tool. If it isn't, take the opportunity to address the underlying issues using the best practices in this handbook.

Don't create social media presences for individual missions, exercises, and events. Instead, coordinate with relevant commands and provide them content that is optimized — both written and visually.

PRIVATE/CLOSED GROUPS.

Not recommended for units. Units should not be publicly releasing information that cannot be seen by all. Closed, private, and unlisted social media groups may sound appealing since they appear to offer a sense of privacy; however, never assume anything on the internet is truly private. People can screenshot and share information from the private/closed group with a wider audience.

IF SOCIAL MEDIA IS RIGHT FOR YOUR COMMAND

HAVE A STRATEGY.

What do you want to do with your account? It may be:

- Share unit updates (for example, "Marines recently concluded training in 29 Palms where they refined X, Y, and Z skills." Best practice: Make the post once the movement/evolution is complete, i.e. share what the unit did, not what the unit is going to do.)
- Highlight accomplishments (awards, promotions, retirements, etc.)
- Amplify media coverage, when appropriate. (Did media or COMMSTRAT cover your event or one of your Marines' accomplishments? Share the coverage on your account.)
- Interact with specific publics. (If you are considering online "town halls" or Q&A sessions, be prepared to answer the tough questions.)

- Use your authentic voice. (Communicate official positions and facts, not opinions or emotions.)

- Answer questions and respond to comments, but don't engage trolls (*see page 12*).

- Interact regularly — at least twice a week. (Engagement depends on the platforms, i.e., for Twitter you should post 1-2 times a day.)

- Don't chase clicks or likes, or try to "go viral". Content that goes viral more often than not does not align with core values.

- Connect with other Marine Corps leaders and commands; support their content when appropriate. Leverage existing discussions as an entry point for your messages.

ADVERSE INCIDENTS

The time to start using social media is not during a crisis. To build credibility, you need to establish a social media presence before then. The better you are at providing good information and engaging your audience, the faster your following will grow.

The best course of action during a crisis is to leverage existing social media presences. If you have a regularly updated channel of communication before a crisis, then your audiences will know where to find information online. Do not make your audience search for information. For example, if your command is preparing for severe weather, tell your audience where they should go for the latest information.

CASUALTIES

When personnel are killed or injured/wounded, it's hard to control the flow of information distributed through social media platforms. Reporters may look at command, Marine, Sailor, civilian and/or family members' social media to get more information. It's important that privacy settings be regularly reviewed to be as restrictive as practical.

It's vitally important to know that the identity of a casualty should not be discussed on social media until it's been released. No casualty information on deceased military or DoD civilian personnel may be released to the media or the general public until 24 hours after the notification of the next of kin. In the event of a multiple-loss incident, the start time for the 24-hour period commences upon the notification of the last family member.

ALTERNATIVES

If your command wants to share information or content privately, social media is not your solution. Social media is never the right venue for sharing sensitive information. If you have sensitive information you want to limit to a specific group, consider one of the Marine Corps' private portals that require a Common Access Card.

If the information or content is to be shared only with family members, consider using a dial-in family line or conveying it through the deployment readiness coordinator (DRC), emails, or family readiness group meetings.

If the information or content is to be shared with the local community, but the command is not subordinate to Marine Corps Installations Command, contact the base COMMSTRAT officer.

If you have information or content that does not regularly change, consider the command's public website.

PROCEDURES FOR ESTABLISHING A COMMAND SOCIAL MEDIA ACCOUNT

STEP 1
Is the social media site (or Internet-based capability) free or paid? If free, continue to step 2. If paid, speak with your local Regional Contracting Office. The RCO is responsible for coordinating Federal-compatible terms of service agreements for paid products.

STEP 2
Ensure the social media site has a Federal-compatible terms of service agreement. Your SJA and contracting office representative can assist with validating this requirement. [Ref: *https://go.usa.gov/xnG7A*]

STEP 3
Obtain approval from your Commanding Officer or Public Affairs Officer (COMMSTRAT). The release authority must approve an official social media site before it can be registered. [Commanding Officers have release authority for their unit only.]

STEP 4
Obtain an appointment letter, in writing, from the Commanding Officer (or individual with by direction authority) designating you as an administrator for the official use of the social media site. [Ref: SECNAVINST 5720.44C CH-1]

STEP 5
It is recommended that an organizational mailbox be established before a government employee registers the new social media site for purposes of providing a non-user specific method of managing the new social media account.

STEP 6
A government employee registers the new social media account and accepts the terms of service agreement on behalf of the Federal government and command.

STEP 7
Register the social media site in the USMC social media directory at *https://www.marines.mil/News/Social-Media* after it has been established.

STEP 8
Ensure a posted disclaimer is published on your new social media site identifying the site as an official site and disclaiming any endorsement. Ensure the terms of participation and posting guidelines are published (or linked to) from your social media site. [Ref: Sample disclaimer, terms and guidelines are available at *https://go.usa.gov/xADpy*]

STEP 9
Establish a social media inspection log or spreadsheet to provide documentation that you inspected all posted content to ensure compliance with the permitted content policy outlined in SECNAVINST 5720.44C CH-1. In accordance with MCO 3070.2A, the command must inspect the social media site's posts for compliance at least quarterly. [Ref: MCO 3070.2A]

STEP 10
It is encouraged that you provide your command COMMSTRAT with access to your social media site to assist with management and monitoring of posted content. In the event of inadvertent disclosure of prohibited content, COMMSTRAT will be able to take immediate action on behalf of the command.

ACCOUNT SECURITY

FACEBOOK

Official Marine Corps Facebook pages must be attached to individuals' Facebook profiles. Don't use a generic Facebook profile; this frequently leads to commands losing access to their pages. Instead, your designated page administrator will use his or her personal Facebook account to manually authorize specific Facebook users to manage the official page. The administrator should grant access to multiple users to minimize the chance of permanently losing access to the page. Once the individual is granted access, updates to the command's Facebook page will be posted as the command's page and not the individual's profile.

What's often blamed on social media hacking is rooted in poor account management: easy-to-guess passwords; passwords that aren't changed regularly or after personnel depart; or lazy device security, such as unlocked computers or mobile devices. Fortunately, these risks can be mitigated.

Even if your password is strong, adversaries may still be able to gain access to your accounts through weak privacy options or third-party access. Carefully look at your security options on each platform to minimize the possibility of unwanted entry. Providing a third-party app or plug-in access to one of your social media accounts can seem like a good idea, but if one of those third-party apps is compromised, your account likely will be as well. Many of those apps and plugins are written by unknown third parties who may use them to access your data and friends. Be conservative about granting third-party apps access, and diligently review who has access to your accounts and eliminate apps you aren't familiar with or no longer use.

If you suspect your command's account has been hijacked or vandalized, follow these steps: Timing is critical in these initial minutes.

- Complete a support request through the social media site. Simultaneously, notify your higher command's COMMSTRAT and your command's security officer. Then, immediately contact Communication Directorate at 703-614-8010 and request assistance from the digital media team.
- Change all other social media passwords. Even if you think the security breach is limited to the

one account, it's prudent to change the passwords of all other social media accounts. If you've lost control of other accounts, contact those platforms immediately as well as Communication Directorate. You should also change the passwords on your personal accounts.

- If you don't have access to your account yet, use other accounts to alert your online community of the breach.
- Once you've regained control of your account, change your password and screen shot the unauthorized content before deleting it.

BLOCKING

The Marine Corps may not block individual social media accounts from official Marine Corps social media sites; however, the Marine Corps may delete comments that constitute a violation of law, regulation, or the Marine Corps' Terms of Use. The Marine Corps may also refer offensive comments to the Social Media Service Provider to consider enforcement of their own Terms of service.

The First Amendment does not permit a public official who utilizes a social media account for all manner of official purposes to exclude persons from an otherwise open online dialogue because they expressed views with which the official disagrees. That said, not all speech is protected under the First Amendment. From 1791 to the present, examples include obscenity, defamation, fraud, incitement, and speech integral to criminal conduct.

Comments posted on official Marine Corps social media sites that constitute a violation of law, regulation or the Marine Corps' Terms of Use may be removed if not needed for evidentiary purposes.

Comments posted by service members that constitute a violation of law or regulation should be referred to the command of the service member who posted the comment or the cognizant DoD law enforcement agency for appropriate action.

Comments posted on official Marine Corps social media sites that constitute a violation of the Terms of service of the Social Media Service Provider may be referred to the Service Provider for their own review and possible enforcement of the Terms of service.

USMC SOCIAL MEDIA RESPONSE GUIDE

DISCOVER

SOCIAL MEDIA POSTING

Has someone discovered a post about the organization? Is it positive or balanced?

YES / NO

EVALUATE

CONCURRENCE

A factual and well-cited response, which may agree or disagree with the post, yet it is not factually erroneous, a rant or rage, bashing or negative in nature. You can concur with the post, let it stand or provide a positive review. Do you want to respond?

NO

LET IT STAND

Let the post stand—no response.

YES

"TROLLS"

Is this a site dedicated to bashing and degrading others?

NO / YES

MONITOR THE SITE

Avoid responding to specific posts, monitor site for relevant information and comments. Notify headquarters.

"RAGER"

Is the posting a rant, rage, joke or satirical in nature?

NO

"MISGUIDED"

Are there erroneous facts in the posting?

YES

FIX THE FACTS

Do you wish to respond with factual information directly?

YES

RESTORATION

Do you wish to rectify the situation and act upon a reasonable solution?

NO

"UNHAPPY CUSTOMER"

Is the posting a result of a negative experience?

YES

NO

RESPOND

SHARE SUCCESS

Do you wish to proactively share your story and your mission?

FINAL EVALUATION

Write responses for current circumstances only. Will you respond?

YES

RESPONSE CONSIDERATIONS

TRANSPARENCY
Disclose your Marine Corps connection.

SOURCING
Cite your sources by including hyperlinks, images, video, or other references.

TIMELINESS
Take time to create sound responses. Don't rush.

TONE
Respond in a tone that reflects highly of the Marine Corps standards.

INFLUENCE
Focus on the most appropriate sites related to the Marine Corps.

INTERACTING WITH THE PUBLIC

Do not friend, follow, or like public users proactively; however, your unit may accept friend requests from public users. Exceptions can be made for following other U.S. federal, state, local, and tribal government agencies, professional associations, or other organization as appropriate.

BOTS

A bot is an automated account run by software capable of posting content or interacting with other users. Some bots pretend to be humans, while others don't. Bots are especially prevalent on Twitter.

In February 2018, Twitter announced changes to its Application Programming Interface that would reduce the ability of services that allow links and content to be shared across multiple accounts, which would affect bots. Yet, bots continue to proliferatle. Be aware that some bots are part of a botnet, or a network of bots that tweet in a coordinated manner. These bots often share the same verbatim tweets and sometimes operate to get specific hashtags trending.

POTENTIAL INDICATORS OF BOTS

- **ANONYMITY.**
  The less personal information available on account, the more likely it belongs to a bot. Look for user names that seem to contain too many numbers and generic profile photos. Perform a reverse image search to see if multiple accounts use the same profile photo.

- **ACTIVITY.**
  Bots frequently engage in suspicious activity. A bot account may have only one tweet with a very high level of engagement, or send out a large number of tweets in a short period of time. Divide the number of tweets by the number of days the account has been active to see how frequently it posts. According to the Atlantic Council's Digital Forensic Research Lab, more than 72 tweets per day is suspicious, and over 144 tweets per day is highly suspicious.

- **AMPLIFICATION.**
  Most bots exist to amplify content. On a typical bot timeline, there will be lots of retweets, word-for-word copied-and-pasted headlines, and/or shares of news stories without additional comment. There is little original content on a bot account.

You can report bot accounts on Facebook, Twitter, Instagram and YouTube. If you're inundated with comments from bot accounts on a particular post, consider posting one comment with factual information and a source to dispel disinformation.

GUIDANCE FOR COMMANDERS

SETTING THE STANDARD FOR ONLINE CONDUCT

As a Marine leader, you must lead by example. You must show your Marines, Sailors, and Marine civilians that improper or inappropriate online behavior is not tolerated and must be reported if experienced or witnessed. When it comes to your position, your conduct online should be no different from your conduct offline, and you should hold your Marines, Sailors, and civilians to that same standard.

Understanding how Marines conduct themselves on social media is critical to providing guidance on how to behave and what expected standards are. Always consider:

- How often do you emphasize appropriate online behavior?
- Have you asked COMMSTRAT personnel to provide social media training?
- Are you prepared to respond to a public, negative incident created by one of your Marines' inappropriate online behavior?
- Do your family members understand how to be safe and appropriate on social media?
- Talk about OPSEC so your Marines and Sailors understand what can and cannot be shared.

If evidence of a violation of command policy, Uniform Code of Military Justice (UCMJ), or civil law by one of your Sailors or Navy civilians comes to your attention from social media, then you can act on it just as if it were witnessed in any other public location. Additionally, pursuant to Marine Corps regulations, you have an affirmative obligation to act on UCMJ offenses you observe. This adds an ethical wrinkle to friending or following your subordinates; the key is for you to maintain the same relationship with them online as you do at work, and to be clear about that.

PERSONAL ACCOUNTS

In addition to the guidance provided to all Marines below, note that your position lends additional authority to your posts. Carefully consider the level of detail used when posting information anywhere on the internet.

Reinforce OPSEC best practices, such as limiting the information you post about yourself, including names, addresses, birthdates, birthplaces, local towns, schools, etc. Small details can be aggregated to reveal significant information that could pose a threat.

Additionally, adversaries can see what you post. They can give extra weight to what information you share based on your current position. For example, if you are the CO of unit X, and you know your unit will soon receive new equipment, and you post about it on social media (Facebook, LinkedIn, Instagram, etc.)...you have assisted the adversary's intelligence collection activities.

GUIDANCE FOR ALL MARINES

In general, the Marine Corps views social media sites positively, and respects your rights as Americans to use them to express yourself. That acknowledged, by the nature of your profession, you are always on the record and you represent our core values. You are a Marine 24-hours a day and 365 days a year. Even if you state you are not representing the Marine Corps, you can be perceived as doing so because you are a Marine.

What happens online stays online and can have real-world impacts in the moment and years after.

When you're online, you're in public — so act like it. Don't do or say anything online you wouldn't do or say in public. Keep relationships and personal life private. Treat everyone online how you'd like to be treated. The "Golden Rule" applies even online.

There's no such thing as complete anonymity online. "My user name is B@sMrinEvr, no one will figure out who I am." Wrong. The people you know will recognize you. Google, Amazon, and other online services designed to capture your online habits to optimize your experience may recognize you.

Before you hit send, stop and think. The things you say matter. Images can be taken out of context. Cool off before responding to messages in anger. You'll never agree with everyone online. Respect others' opinions. Anyone, anywhere could see what you post.

The internet doesn't forget. It's very easy for bad actors to save a screenshot, download an image, or do something else to make sure a moment online lasts an eternity. Anything shared online, although intended to be private and confidential, has the possibility to become public — if it's best left unsaid, don't say it. If you don't want it shared, don't post it.

Protect your privacy and your friends' privacy too by not sharing without their permission.

Unless you're prepared to attach that post, text, or photo to your next college application, security clearance package, or resume, again, stop and think before you post.

Anything posted on the internet is permanent. Through the use of publicly available online tools, data can be recovered and used against you.

PARTICIPATING IN ONLINE CONVERSATIONS

GENERAL RULES.

You are personally responsible for what you say and post on social networking services and any other medium. Consider how a post can be interpreted by the public. Be cautious

about crossing the line between funny and distasteful. If you have doubts about whether you should post something, err on the side of caution. Maintain appropriate communication and conduct with officer and enlisted personnel, peers, superiors and subordinates (to include civilian superiors and subordinates).

NO CLASSIFIED INFORMATION.

Do not post classified or sensitive information (for example, troop movements, force sizes, weapons details, etc.) If in doubt, ask. Security is at the source. Pay attention to what's in the background of photos/videos.

REPLACE ERRORS WITH FACTS, NOT ARGUMENTS.

When you see misrepresentations made about the Marine Corps in social media, you may certainly point out the error. Do so with respect and with the facts. When you speak to someone with an adversarial position, make what you write/say factual and not disparaging. Avoid arguments.

ADMIT MISTAKES.

Be the first to respond to your own mistakes. If you make an error, be up front about your mistake and correct it quickly.

AVOID THE OFFENSIVE.

Do not post defamatory, libelous, vulgar, obscene, profane, threatening, racially and ethnically divisive, or otherwise offensive or illegal information or material.

WRITTEN PERMISSION.

Do not post any information or other material protected by copyright without the written permission of the copyright owner.

TRADEMARKS — DON'T BREACH.

Do not use any words, logos, or other marks that would infringe upon the trademark, service mark, certification mark, or other intellectual property rights of the owners of such marks without the permission of the owners.

DON'T VIOLATE PRIVACY.

Do not post any information that would infringe upon the proprietary, privacy, or personal rights of others.

AVOID ENDORSEMENTS.

Do not use the Marine Corps name to endorse or promote products, opinions, or causes. This includes posting responses to online challenges while in uniform or other attire that identifies you as a Marine.

DON'T SOLICIT.

No Marine may solicit gifts or prizes for command events in any capacity — on duty, off duty or in a personal capacity.

NO IMPERSONATIONS.

Do not forge or otherwise manipulate identifiers in your posts in an attempt to disguise, impersonate, or otherwise misrepresent your identity or affiliation with any other person or entity. Impostor accounts violate most social media platforms' terms of service.

IMPOSTER ACCOUNTS.

Help us search for impostors and report them to the social media platform. The impersonation of a senior Marine Corps official, such as a general officer or a commanding officer, should also be reported, via your COMMSTRAT channels, to Headquarters Marine Corps, Communication Directorate.

USE DISCLAIMERS.

Identify to readers of personal social media accounts that the views you express are yours alone and that they do not necessarily reflect the views of the Marine Corps. Use a disclaimer such as, "The postings on this site are my own and don't necessarily represent Marine Corps positions, strategies, or opinions."

STAY IN YOUR LANE.

Discussing issues related to your personal experiences is acceptable, but do not discuss areas of expertise for which you have no background or knowledge.

DON'T LIE.

Credibility is critical, without it, no one cares what you have to say. It's also punishable by the UCMJ to give a false statement.

LINK.

You may provide a link from your accounts to a Marine Corps site.

USE COMMON SENSE.

This is the bottom line. If you don't want to read about it/see it in the news or be asked about it by people whom you respect — don't say it, don't do it, don't post it. Your words and images can go out to thousands and possibly millions of people around the world instantly, and once it's out there, it's out there for good. Don't go viral for the wrong reasons.

YOUR FIRST AMENDMENT RIGHTS

Marines and Sailors using social media are subject to the UCMJ and Marine Corps/Navy regulations at all times, even when off duty. Commenting, posting, or linking to material that violates the UCMJ or Marine Corps/Navy regulations may result in administrative or disciplinary action, to include administrative separation, and may subject Marine Corps civilians to appropriate disciplinary action.

Applicable UCMJ and federal criminal law violations include, for example:

Applicable to Members of the Armed Forces

- Article 82. Solicitation
- Article 88. Contempt toward officials
- Article 89. Disrespect toward superior commissioned officer
- Article 91. Insubordinate conduct toward warrant officer, noncommissioned officer, or petty officer
- Article 92. Failure to obey order or regulation
- Article 117. Provoking speeches or gestures
- Article 134. General Article

Applicable to All Persons

- 18 U.S.C § 2385. Advocating overthrow of the Government
- 18 U.S.C § 2387. Activities affecting the Armed Forces generally
- 18 U.S.C § 2388. Activities affecting the Armed Forces during war

Service members may not actively advocate supremacist, extremist, or criminal gang doctrine, ideology, or causes, including those that advance, encourage, or advocate illegal discrimination based on race, creed, color, sex, religion, ethnicity, or national origin. Service members may not advance, encourage, or advocate the use of force, violence, or criminal activity or otherwise advance efforts to deprive individuals of their civil rights.

Per MCO 5354.1E — Marine Corps Prohibited Activities and Conduct Prevention and Response Policy, Marines are prohibited from engaging in harassment (to include sexual harassment); unlawful discrimination, and abuse (specifically, hazing, bullying, ostracism, retaliation (with the exception of restriction and reprisal); wrongful distribution or broadcasting of intimate images; and, certain dissident and protest activity (to include supremacist activity). This includes online conduct.

POLITICAL ACTIVITY

Marines may generally express their personal views about public issues and political candidates on internet sites, including liking or following accounts of a political party or partisan candidate, campaign, group, or cause. If the site explicitly or indirectly identifies Marines as on active duty (e.g., a title on LinkedIn or a Facebook profile photo), then the content needs to clearly and prominently state that the views expressed are the Marine's own and not those of the U.S. Marine Corps or Department of Defense.

Marines may not engage in any partisan political activity such as posting direct links to a political party, campaign, group, or cause on social media — this is considered equivalent to distributing literature on behalf of those entities, and is prohibited.

Similarly, as a leader, you cannot suggest that others like, friend or follow a political party, campaign, group or cause.

Marines should be aware of the limitations that exist when it comes to participation in political activity as well as DOD support to political campaigns.

ACTIVITY	PERMITTED	PROHIBITED
PARTICIPATE IN ANY INTERVIEW OR DISCUSSION AS AN ADVOCATE FOR OR AGAINST A PARTY, CANDIDATE, OR CAUSE.		▲
GENERALLY EXPRESS YOUR PERSONAL VIEWS ON PUBLIC ISSUES OR POLITICAL CANDIDATES VIA SOCIAL MEDIA PLATFORMS MUCH THE SAME AS IF YOU WROTE A LETTER TO THE EDITOR OF A NEWSPAPER.	▲	
PARTICIPATE IN PARTISAN POLITICAL ACTIVITY		▲
FOLLOW, FRIEND, OR LIKE A POLITICAL PARTY OR CANDIDATE RUNNING FOR PARTISAN OFFICE.	▲	
POST OR SHARE CONTENT FROM A POLITICAL PARTY OR CANDIDATE RUNNING FOR PARTISAN OFFICE		▲
COMMUNICATE CONTEMPTUOUS WORDS AGAINST THE PRESIDENT, VICE PRESIDENT, DEFENSE SECRETARY, DEFENSE DEPUTY SECRETARY, SERVICE SECRETARIES, OR GOVERNOR AND LEGISLATURE OF ANY STATE WHERE YOU ARE LOCATED OR PERFORMING DUTY.		▲

REPORTING IMPROPER BEHAVIOR

Anyone who experiences or witnesses incidents of improper online behavior should promptly report it.

Reports can be made to the chain of command. Additional avenues for reporting include Equal Employment Opportunity offices, the Inspector General, Sexual Assault Prevention and Response offices and the Naval Criminal Investigative Service.

NCIS encourages anyone with knowledge of criminal activity to report it to their local NCIS field office directly or via web or smartphone app at *https://www.ncis.navy.mil/Resources/NCIS-Tips/*.

OPERATIONS SECURITY

OPSEC violations commonly occur when personnel share information with people they don't know well or if their social media accounts have loose privacy settings. A good practice is to limit the information you and your families post including addresses, birthdates, birthplaces, local towns, schools, etc. Small details can be aggregated to reveal significant information that could pose a threat.

When posting, ask yourself what could a person do with this information? Could it compromise my safety or the safety of my family or my unit?

DO	DON'T
Turn off geotagging and location-based services. (Geotagging adds location-based information to content such as photographs, videos, websites, and messages. It is the equivalent of adding a 10-digit grid coordinate. Some devices and services may automatically embed geotags into content.)	Post details about your unit's mission or security procedures, or announce locations and times of deployments.
Maximize your security settings and use two-step verification, if available. Default security and privacy settings may change — with or without notice, so frequently review your desired settings.	Release information about the death or injury of a service member before the information is officially released. Next of kin should not learn of deaths or grievous injuries from social media. Post images of damaged equipment or gear.
Closely review content before posting to ensure sensitive or personal information is not released (e.g. troop locations, equipment, tactical unit details, and numbers of personnel).	Share personnel transactions (e.g. pay information, power of attorney, wills, or deployment information). Post unit morale or personnel issues.

ACCOUNT SECURITY

UPDATES.

Keep your technology up to date (computer, phone, tablet, etc.). Whenever you get a software update at work or at home, run it. These are typically patches for recent security vulnerabilities.

TRACKING.

Beware of tracking your location. Many social media platforms allow for "check in" and share your location, or automatically add location information to photos and posts.

PUBLIC WIFI.

Avoid using public WiFi. With a public internet connection, you run the risk of being hacked. If you must use a public Wi-Fi connection, here are some things you can do to be safer:

- Don't shop or go to your bank accounts on public Wi-Fi.
- Only go to sites that use a secure connection (indicated by an "HTTPS" in their web address). This means they use encryption to protect your information.
- Use a Virtual Public Network (VPN). This — often paid-for — service provides a more secure connection.
- If available, use two-factor authentication. Anyone trying to pretend to be you, won't be able to access your accounts because they won't have your phone or computer.

LOGIN NOTIFICATIONS.

Set login notifications on all your accounts so when someone tries to login from a new location, you get an email and can take proactive action if necessary.

BACKUP YOUR DATA.

Frequently backup data at home and in the workplace. Many commercial cloud and physical storage devices will encrypt data automatically for extra protection.

PASSWORDS.

Use strong password protocols. The best password is a string of at least 12-15 random characters containing numbers, upper- and lower-case letters and symbols. Don't try and remember all passwords for all platforms and devices. Use a password manager. Don't share passwords. Don't use the same password for more than one site or device. Never reuse an old password. Put passwords on all of your devices, and put a strong password on your network at home. This includes changing the default password on personal routers at home.

SECURITY QUESTIONS.

Answer security questions creatively. Sites often have security questions that use personal information to help you recover or reset a password. For example, hackers can deduce the answers from social media accounts to make attempts at changing an individual's password, locking them out, and stealing valuable data. You can make this harder by either giving a different response to the question or padding your response with something no one knows but you, such as adding a special character at the end of a response.

BE A CYBER SENTRY

There are many tactics people may use to trick others into providing information or granting access to that information through social networking venues.

Once information is posted to a social networking site, it is no longer private. The more information you post, the more vulnerable you may become. Even when using high security settings, friends or websites may inadvertently leak your information. Personal information you share could be used to conduct attacks against you or your associates. The more information shared, the more likely someone could impersonate you and trick one of your friends into sharing personal information, downloading malware, or providing access to restricted sites.

Predators, hackers, and foreign state actors troll social networking sites looking for information or people to target for exploitation. Information gleaned from social networking sites may be used to design a specific attack that does not come by way of the social networking site.

Although, not exhaustive, below are some of these tactics and suggested ways to mitigate online social networking risks.

BAITING

Someone gives you a USB drive or other electronic media that is preloaded with malware in the hope you will use the device and enable them to hack your computer.

Do not use any electronic storage device unless you know its origin is legitimate and safe. Scan all electronic media for viruses before use.

CLICK-JACKING

Concealing hyperlinks beneath legitimate clickable content which, when clicked, causes a user to unknowingly perform actions, such as downloading malware, or sending your ID to a site. Numerous click-jacking scams have employed Like and Share buttons on social networking sites.

Disable scripting and iframes (another webpage inserted so it appears to be one page) in whatever Internet browser you use. Research other ways to set your browser options to maximize security.

CROSS-SITE SCRIPTING (XSS)

Malicious code is injected into a benign or trusted website. A Stored XSS Attack is when malicious code is permanently stored on a server; a computer is compromised when requesting the stored data. A Reflected XSS Attack is when a person is tricked into clicking on a malicious link; the injected code travels to the server then reflects the attack back to the victim's browser. The computer deems the code is from a "trusted" source.

Turn off "HTTP TRACE" support on all webservers. Research additional ways to prevent becoming a victim of XSS.

DOXING

Publicly releasing a person's identifying information including full name, date of birth, address, and pictures typically retrieved from social networking site profiles.

Be careful what information you share about yourself, family, and friends (online, in print, and in person). Soliciting for personal information can take innocent forms, such as, "See what your band name is" followed by a graphic showing random words next to months and dates. You post what your "band name" is and now everyone knows your date of birth.

ELICITATION

The strategic use of conversation to extract information from people without giving them the feeling they are being interrogated.

Be aware of elicitation tactics and the way social engineers try to obtain personal information.

PHARMING

Redirecting users from legitimate websites to fraudulent ones for the purpose of extracting confidential data. (E.g.: mimicking bank websites.)

Watch out for website URLs that use variations in spelling or domain names, or use ".com" instead of ".gov", for example. Type a website's address rather than clicking on a link.

PHISHING

Usually an email that looks like it is from a legitimate organization or person, but is not and contains a link or file with malware. Phishing attacks typically try to snag any random victim. Spear phishing attacks target a specific person or organization as their intended victim.

Do not open email or email attachments or click on links sent from people you do not know. If you receive a suspicious email from someone you know, ask them about it before opening it.

PHREAKING

Gaining unauthorized access to telecommunication systems.

Do not provide secure phone numbers that provide direct access to a Private Branch Exchange or through the Public Branch Exchange to the public phone network.

SCAMS

Fake deals that trick people into providing money, information, or service in exchange for the deal.

If it sounds too good to be true, it is most likely a scam. Cybercriminals use popular events and news stories as bait for people to open infected email, visit infected websites, or donate money to bogus charities.

SPOOFING

Deceiving computers or computer users by hiding or faking one's identity. Email spoofing utilizes a sham email address or simulates a genuine email address. IP spoofing hides or masks a computer's IP address.

Know your co-workers and clients and beware of those who impersonate a staff member or service provider to gain unit or personal information.

GUIDANCE FOR FAMILIES

As a family member, you are integral to the success of the Marine Corps. Without your support, Marines wouldn't be able to accomplish the great work they do every day. The Marine Corps stories you share on social media help maintain the morale of Marines and educate the public about the Marine Corps.

To use social media safely, it's important for Marines and their families to identify and safeguard critical information about military operations. Be cautious about sharing personal information or communicating with people over social media. Posting too much information could jeopardize the security of Marines and missions. If you wouldn't want to see the information on the news, do not post it on the internet.

Social content shared by Marines and families is a target for those looking to gain access to sensitive information in order to impersonate, blackmail, or intimidate.

Don't post the exact whereabouts and activities of deployed Marines.

Be general about the dates and locations concerning a Marine's trip arrival and departure.

Don't publicly post exactly how long your Marine will be gone on a trip or deployment.

Don't make your vacation dates public on social networks. Criminals may track your activities and know exactly when to break into your home while you're on vacation.

Be careful about publicly posting children's photos, names, schools, ages, and schedules.

Let children know they should seek help for cyber-bullying.

You're encouraged to use social media to engage in support networks, such as spouse's clubs, event committees, child care groups, or local civic activities. These groups are not considered official Marine Corps social media, and you don't need permission to form a group of your own. You may want to limit the membership and visibility of the group to help protect the information exchanged. Even if the membership and visibility is limited, never discuss sensitive information online.

You may also want to follow the main Marine Corps social media accounts or your local installation's accounts for the latest information on the work your Marine does. You can help support their specific missions by sharing their social media content and experiences with your followers and friends.

MEDIA LITERACY

This section is adapted from Cornell University Library's "Fake News, Propaganda and Misinformation: Learning to Critically Evaluate Media Sources" (2020) and includes excerpts from it.

There is no shortage of information, and accuracy can be hard to gauge. Misinformation is unintentionally inaccurate. Disinformation is intentionally inaccurate. Critical thinking skills are the best defense against mis/disinformation. It is important for Marines to be critical consumers of information, to not fall for disinformation campaigns, to recognize when misinformation may be present, and to not contribute to the spread of either.

BE CURIOUS.

Independently verify the source and the information. Is more than one source reporting the same thing, or is this the only place you have seen the information?

BE REFLECTIVE.

Pause, reflect, and investigate — especially if you immediately have an emotional reaction, which is the primary goal of fake news producers.

ACTIVELY INVESTIGATE YOUR NEWS SOURCES.

Select news sources known for high-quality, investigative reporting. Search for these sources directly. Social media algorithms present information that reinforces your current views, not a balanced view.

LOOK FOR IN-DEPTH COVERAGE.

Look for lengthy articles — long-form reporting — that capture some of the complexity of topics and events. One or two paragraphs is not sufficient.

USE CARE BEFORE SHARING NEWS CONTENT ON SOCIAL MEDIA.

Pause and reflect on news sources that arouse strong emotions, positive or negative.

SO, WHAT IS FAKE NEWS?

Fake news is fabricated information, which mimics news media content in form, but not in organizational process or intent. It overlaps with other information disorders, such as misinformation (false or misleading information) and disinformation (false information that is purposely spread to deceive people).

In order to be media literate, you need to be aware of other questionable sources of information:

- Deepfakes use software to create events that never happened or distort a person's statements.
- Satire uses humor, irony, exaggeration, ridicule, satire, and false information to comment on current events.
- State-sponsored news is often the source of propaganda in repressive states operating under government sanctions.
- Junk science promotes discredited conspiracy theories, naturalistic fallacies, and scientifically false or dubious claims.
- Clickbait provides generally credible content, but uses exaggerated, misleading, or questionable headlines, social media descriptions, and/or images.

HOW TO SPOT FAKE NEWS

CONSIDER THE SOURCE
Click away from the story to investigate the site, its mission and its contact info.

READ BEYOND
Headlines can be outrageous in an effort to get clicks. What's the whole story?

CHECK THE AUTHOR
Do a quick search on the author. Are they credible? Are they real?

SUPPORTING SOURCES?
Click on those links. Determine if the info given actually supports the story.

CHECK THE DATE
Reposting old news stories doesn't mean they're relevant to current events.

IS IT A JOKE?
If it is too outlandish, it might be satire. Research the site and author to be sure.

CHECK YOUR BIASES
Consider if your own beliefs could affect your judgement.

ASK THE EXPERTS
Ask a librarian or consult a fact-checking site.

GUIDANCE SUMMARY

DOD INSTRUCTION 8170.01.
ONLINE INFORMATION MANAGEMENT AND ELECTRONIC MESSAGING. (2 JANUARY 2019) *HTTPS://WWW.ESD.WHS.MIL/PORTALS/54/DOCUMENTS/DD/ISSUANCES/DODI/817001P.PDF*

ENDORSEMENTS

Do not imply DoD endorsement in any manner for any specific non-U.S. Government service, facility, event, or product.

Do not accept remuneration of any kind (e.g., payment, reimbursement, reduced prices, gifts) in exchange for advertising, acknowledgement, or endorsement without specific authority to do so.

SURVEYS

Information collection via online surveys, forms, or other solicitations is subject to DoD 5240.1-R and 7750.07-M, DoDD 5148.13, DoDIs 1000.30, 1100.13, 7750.07, and 8910.01, DoD Manual 5240.01, and Chapter 91 of Title 15, U.S.C., as applicable to the intent or target audience of the collection.

Specific applications of these regulations are governed by distinct policies and guidelines. The April 7, 2010 OMB Memorandums provide specific additional guidance to help determine when a collection is governed by or subject to the named sources.

COPYRIGHT

Proper attribution must be made for all copyrighted material.

Post a clear disclaimer detailing the copyrights retained by USG or non-USG contributors and identify the specific copyrighted work(s) (e.g., information, image, video, sound, design, code, template, service, technology) when placing copyrighted material on electronic messaging services.

ALTERING IMAGERY

Do not alter official DoD imagery beyond the allowances specified in DoDI 5040.02.

HYPERLINKS

Use hyperlinks only to information or services related to the performance of the DoD component's function or mission and the purpose of the electronic messaging service.

Verify all external hyperlinks to ensure continued provision of the hyperlink quality (i.e., correct address and objectivity, utility, and integrity of the content) intended by the DoD Component and expected by users.

External Hyperlink Disclaimer

"The appearance of hyperlinks does not constitute endorsement by the U.S. Marine Corps of non-U.S. Government sites or the information, products, or services contained therein. Although the [insert sponsoring organization] may or may not use these sites as additional distribution channels for Department of Defense information, it does not exercise editorial control over all of the information that you may find at these locations. Such hyperlinks are provided consistent with the stated purpose of this website."

OFFICIAL USE OF NON-DOD-CONTROLLED ELECTRONIC MESSAGING SERVICES

Do not use non-DoD-controlled electronic messaging services to process nonpublic DoD information, regardless of the service's perceived appearance of security (e.g., "private" Instagram accounts, "protected" tweets, "private" Facebook groups, "encrypted" WhatsApp messages).

When engaging in official use of non-DoD-controlled electronic messaging services, DoD organizations should:

- Limit use of non-DoD-controlled electronic messaging services to supplemental communication only. Do not establish or represent official-use accounts or pages as primary sources of DoD information.
- Organizations should provide individuals with comparable alternatives to non-DoD controlled electronic messaging services through the organization's official website or other official means. For example, members of the public should be able to learn about the organization's activities and to communicate with the organization without having to join a third-party social media website.
- If an organization uses a non-DoD-controlled electronic messaging service to solicit feedback, i.e. ask for any information, the organization should provide an alternative government e-mail address where users can also send feedback.

TERMS OF SERVICE (TOS)

If the DoD chief information officer has not signed a Terms of Service agreement for a non-DoD-controlled electronic messaging service, establish a Terms of Service agreement signed at the DoD component level.

The GSA provides Terms of Service templates appropriate for federal government use, which are available at *https://www.digital.gov*, that must be adapted for DoD use if available for the desired service.

PERSONAL USE OF SOCIAL MEDIA

DoD personnel may establish non-DoD-controlled electronic messaging accounts for personal, nonofficial use.

Personal, nonofficial accounts may not be used to conduct official DoD communications for personal convenience or preferences.

DoD personnel may use personal, nonofficial accounts to participate in activities such as professional networking, development, and collaboration related to, but not directly associated with, official mission activities as DoD personnel.

When conducting personal, nonofficial communication, DoD personnel must:

- Avoid the distribution and discussion of nonpublic information or the appearance of official sanction.
- Not disclose nonpublic information, or unclassified information that aggregates to reveal sensitive or classified information.

DoD personnel should use non-mission related contact information, such as personal telephone numbers or postal and e-mail addresses, to establish personal, nonofficial accounts, when such information is required.

DoD personnel who are acting in a private capacity have the First Amendment right to further release or share publicly-released unclassified information through non-DoD forums or social media provided that no laws or regulations are violated.

DoD personnel will not post comments or material that denigrates another military or civilian member of the DoD team.

DODD 1344.10.
POLITICAL ACTIVITIES BY MEMBERS OF THE ARMED FORCES. (19 FEBRUARY 2008) *HTTPS://WWW.ESD.WHS.MIL/PORTALS/54/DOCUMENTS/DD/ISSUANCES/DODD/134410P.PDF*

Members on active duty should not engage in partisan political activity.

Activities not expressly prohibited may be contrary to the spirit and intent of this directive. Any activity that may be reasonably viewed as directly or indirectly associating the DoD or any component with a partisan political activity or is otherwise contrary to the spirit and intention of this directive shall be avoided.

DODI 130018P.
DEPARTMENT OF DEFENSE (DOD) PERSONNEL CASUALTY MATTERS, POLICIES, AND PROCEDURES. (14 AUGUST 2009) *HTTPS://WWW.ESD.WHS.MIL/PORTALS/54/DOCUMENTS/DD/ISSUANCES/DODI/130018P.PDF*

No casualty information on deceased military or DoD civilian personnel may be released to the media or the general public until 24 hours after notifying the NOK regarding the casualty status of the member.

Casualty information on ill or injured Service members or DoD civilians may not be released without the consent of the individual.

SECNAVINST 5720.44C.
DEPARTMENT OF THE NAVY PUBLIC AFFAIRS POLICY AND REGULATIONS. (21 FEBRUARY 2012)

IMAGERY

All content posted to publicly-accessible internet presences, including graphics, photos, video, and multimedia productions, must be carefully reviewed to ensure it meets the standards and requirements for the public release of information.

CAPTIONS

All graphics, photos, video, and multimedia content posted on publicly-accessible DoN internet presences must have a VIRIN and a caption.

PROHIBITED CONTENT AND LINKS

Applies to content and posts on all DoN publicly-accessible internet presences, including but not limited to, command or activity websites, command or activity presences on IbC platforms, and posts made in one's official capacity to IbC presences not owned or managed by the DoN, command, or activity.

- Classified material, "For Official Use Only" information, proprietary information, pre-decisional information, any other form of sensitive but unclassified (SBU) information, or information that could enable the recipient to infer this type of information.

  This includes, but is not limited to, lessons learned or maps with specific locations of sensitive units, ship battle orders, threat condition profiles, etc., activities or information relating to ongoing criminal investigations into terrorist acts, force protection levels, specific force protection measures being taken or number of personnel involved, plans of the day or month.

- Information protected by the Privacy Act of 1974 or the Health Information Portability and Accountability Act of 1996 (HIPPA). Personally identifiable information other than the name, rank or rate, assigned unit (if appropriate for release), and home state of individual service member or civilian employee of the DoN. Other than in official news releases or stories, such identification shall only be made to indicate the single point of contact for a provided service, or when indicating an author of a document, report, or study.

- Identification of immediate family members of DoN personnel by name, including in imagery captions, except for a spouse of a senior leader who is participating in public events such as a ship naming, commissioning, etc. Family member information will not be included in any online biographies.

- Unit or other personnel lists and rosters, charts or directories, which provide the names, addresses, e-mail addresses, and/or telephone numbers of individual unit members.

- Information, other than authorized press releases, about casualties prior to official confirmation that next of kin has been notified and a 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.

- Copyrighted and trademarked material used without the written permission of the copyright or trademark holder.

- Material that is political in nature or that endorses or promotes products, opinions, or causes other than those already officially endorsed by the DoN.
- Any content that may imply endorsement, including links to advertising, promotions, solicitations, or endorsements of products, non-government services, of a political nature, or to commercial entities, charities, or causes. Links to the Combined Federal Campaign and/or the Navy-Marine Corps Relief Society are permitted and encouraged.
- Per DoDI 1015.10, Morale Welfare and Recreation (MWR) activities are allowed to promote and advertise MWR programs, activities and events, and conduct MWR commercial sponsorship and advertising.
- Commercial software or links to commercial software for download except in those cases where the software is unique and required for viewing documents provided within the website's purpose. In these cases, only a text link directly to the vendor's download web page is permitted. The use of corporate logos is prohibited.
- Advertisement for, or sales of, materials or services, such as for an online ship's store selling command memorabilia, ball caps, etc. Commercial sponsorship or advertisements shall not be displayed on publicly accessible MWR and Marine Corps Community Service (MCCS) web presences except as provided in paragraph (9) above.
- Links to additional information regarding MWR sponsored events hosted on non-".mil" domains shall not be displayed on publicly-accessible MWR and MCCS web presences, but may be included on pages accessible only to authorized MWR and MCCS patrons.
- Linking disclaimers when linking to the website of a local, state, or federal government entity.
- Links to the homepages of websites of private sector news media, magazines, publishers, or radio or television stations.
- Links to commercial or copyrighted maps.
- Installation maps displaying the locations of operational commands or force protection facilities. The use or copying of commercial and/or copyrighted maps is prohibited.

PERMISSIBLE CONTENT AND LINKS

- Links to information under the purview of and posted to other military or U.S. Government websites.
- General telephone numbers and non-personalized email addresses for commonly-requested resources, services, and contacts, without individuals' names.

- The names, telephone numbers, and personalized official e-mail addresses of command and activity COMMSTRAT personnel and/or those designated by the commander as command spokespersons may be included in otherwise non-personalized directories, etc.

- Biographies published will not include date of birth, age, current residential street address, or any information about family members. Place of birth, if desired to be included, will be presented as "... is a native of...". Official portraits must be head and shoulders only.

- Due to the public nature of their duties, internet presences may include the official biographies and portraits of: Flag officers, commanders, commanding officers, officers in command, executive officers or deputies, the civilian equivalents of those officers just listed, and command master chief petty officers and senior enlisted advisors or Marine Corps master gunnery sergeants or sergeants major.

- Copyrighted and trademarked material used with written permission from the copyright or trademark holder related directly to the command's primary mission and must be clearly marked that the material is under copyright and by whom. Works prepared by DON personnel as part of their official duties and posted to a command internet presence may not be copyrighted, nor may a DON internet presence itself be copyrighted.

- To specific articles about the DON command or activity in traditional and online media when such linking would be reasonably seen as not an endorsement of the entity to which the link is made.

USE OF MARINE CORPS TRADEMARKS

The Marine Corps reserves the right to review, screen, or license any USMC-themed private-sector product or advertisement to ensure the proposed usage upholds the dignity and reputation of the USMC and to ensure such use does not subject the Marine Corps to discredit or adversely affect the health, safety, welfare, or morale of members of the Marine Corps, or is otherwise objectionable, per Marine Corps Order 5030.3B.

The use of Marine Corps trademarks by third parties for any purpose, including reproduction on merchandise, is expressly prohibited unless the producer enters into a license agreement with, or is otherwise granted permission by, the Marine Corps. Use is governed by the terms of the license agreement (10 U.S.C. §2260).

Except for trademark licenses or other grants of permission, DoD and Marine Corps policy and regulations prohibit use of official Marine Corps markings and symbols in ways that imply endorsement of a commercial entity or activity.

PRODUCED BY
HEADQUARTERS, MARINE CORPS COMMUNICATION DIRECTORATE
PRODUCTION AND ENGAGEMENT
703-614-1887 | socialmedia@usmc.mil

U.S. MARINE CORPS
2021 SOCIAL MEDIA HANDBOOK