UNITED STATES MARINE CORPS
I MARINE EXPEDITIONARY FORCE
U. S. MARINE CORPS FORCES, PACIFIC
BOX 555325
CAMP PENDLETON, CA 92055-5325

5780
COMMSTRAT

JAN 16 2018

POLICY LETTER 13-17

From: Commanding General, I Marine Expeditionary Force
To: Distribution List

Subj: I MARINE EXPEDITIONARY FORCE SOCIAL MEDIA POLICY

Ref: (a) ALMAR 008/17

Encl: (1) Social Media Best Practices

1. Purpose. Establish social media policy to guide Marines and their families through the increased risks found in the interconnectivity and limitless communication provided by social media and other web-based interactive technologies.

2. Information. The world's ability to communicate and share personal information has expanded exponentially with the rise of social media and other web-based interactive technologies. This increase in personal communication capability requires due diligence and oversight at individual and unit levels. I Marine Expeditionary Force (I MEF) recognizes the major role and influence of social media in the lives of individual service members, their families and on a larger, operational level. As a major component in personal communication and interconnectivity, social media training is necessary to preserve information security and to maintain safe and appropriate online networks and forums. I MEF is dedicated to maintaining a cohesive, resilient, and inclusive operational force both on and off-line.

3. Scope. This policy applies to all military, civilian, and contracted support personnel assigned to I MEF and its Major Subordinate Commands (MSC) and elements. Social media includes collaborative tools such as social networking sites, user-generated content, social software, e-mail, instant messaging, and discussion forums. The use of such platforms can be delineated into two categories: professional use and personal use. Professional use refers to the use of social media platforms for professional activities, such as operating official unit pages and accounts. Personal use refers to the use of personal social media accounts for purposes unrelated to unit operations. Professional social media use is most often limited to Communication Strategy (CommStrat) and recruiting Marines, while any service member can use social media personally.

4. Policy. Marines are to follow ref (a) while utilizing social media sites or internet based platforms. Marines must never engage in commentary or publish content on social networking platforms or through other forms of communication that harm good order and discipline or that bring discredit upon themselves, their unit, or the Marine Corps. Furthermore, they must avoid actions online that threaten the morale, operational readiness and security, or public standing of their units, or that compromise our core values. Encl (1) is included to provide an easily digestible document

outlining the appropriate use of social media, yet this document only serves to complement ref (a), not replace it.

5. Certification. Each command or department will ensure their Marines, civilians, and contracted support personnel are informed of this policy, have read and understand ref (a), and are aware of the best practices listed in encl (1). This will also allow Marines to strongly encourage their family members to follow these best practices. Family Readiness Officers will disseminate recommended best practices to I MEF family members.

6. Point of Contact. Contact the Communication Strategy and Operations Office for further guidance on public facing applications and the Information Management Office for internally used applications.

LEWIS A. CRAPAROTTA

Distribution: I/II
Copy to: 3d MAW
1st MarDiv
1st MLG
I MIG
11 MEU
13 MEU
15 MEU

Social Media Best Practices

Nothing on the internet is truly private. Service members and their families must keep this in mind when using social media platforms and know that information that may be intended just for friends and family may not be as protected as originally assumed, or could be forwarded on to unintended recipients. Online content can and will be shared with thousands of people and it is impossible to retract this information once it has entered the public arena. Once anything is online - no matter how private a forum it is assumed to be - it is in the public arena.

Like any other action, be it operational or personal, social media use requires that Marines develop a personal risk management plan. Given the proliferation of social media in daily personal operations, it is often unavoidable. Because of this, Marines and their families need to be hyper aware of the risks to their personal information, operational information, and personal and professional reputations.

The Marine Corps is, above all else, guided by the principles of honor, courage, and commitment. In deed and appearance, service members must keep themselves, I MEF, and the Marine Corps above reproach. The medium and platform for communication may change, but the Marine Corps' standards do not.

Basic Principles

Integrity is one of our most important principles. Avoid writing or posting anything that would embarrass you, the Marine Corps, or compromise anyone's ability to do their job, as outlined in ALMAR 008/17.

Assume that your professional life and your personal life will merge online regardless of your care in separating them.

Despite privacy settings and tools, it is best to assume anything you write, post, exchange, share or receive on any platform is public.

Just as certain partisan political activities are not allowed in the office, you should think carefully before engaging in partisan activities online. Again, assume everything is public. You work for an apolitical, federal organization that supports and defends all Americans and abides by the orders of the President of the United States and federal and state laws. It would be an embarrassment to the Marine Corps and I MEF if someone were to infer that you would choose not to carry out your duties appropriately due to online partisan involvement.

Service members are, unfortunately, also targeted via social media platforms. Adversaries can use them to gather personal information about service members and their families. Individuals wishing to target and manipulate service members will utilize the anonymity often available on social media to do so. These are not reasons to avoid social media, but they are facts that service members need to consider and be aware of when utilizing these platforms.

At the opposite end of the spectrum, Marines may feel comfortable using an alternative persona or hiding behind a username online, taking advantage of the anonymity the internet may seem to afford them. This is ill advised. No matter how hard you try, information you disclose can still identify you as a service member. Between geotagging, IP addresses, and other more advanced means, third parties can determine who and where you are. It also goes completely against the basic principles of honor, courage, and commitment to try and mask your identity in order to degrade others and conduct yourself in a less than acceptable manner on the internet.

The method and medium of communication is constantly changing, especially as new social media and online platforms develop. While these things change, I MEF's standards do not; there should never be a question of how to represent yourself, I MEF, and the Marine Corps online. Seek guidance from your chain of command if you are unsure of how our standards apply to online conduct.

Platform Specific Guidance

It is imperative that when you utilize social media platforms you realize that you and the content you exchange on them are subject to their terms of service. This can have legal implications, since the site or application in question will have access to and control over everything you have disclosed, posted or exchanged on that platform.

It is also important to recognize that while most platforms have what seem to be robust privacy settings, anyone can take a "screenshot" and capture what you have shared with them in a photo file. They can then share and send that photo to anyone, who can in turn send it to anyone and the information you originally assumed was private is now open to the world. Nothing is private.

Facebook

Facebook is the most popular social media platform to date and the one you and your family probably use the most often. Despite robust privacy settings, Facebook will collect and track your usage and information to better tailor marketing and advertising efforts directed at you. This information is kept by Facebook, and the availability of it to third-party review is often a point of contention in congressional legislation. You do not own this information and should assume none of it is permanently, if at all, private.

Facebook also frequently updates their privacy settings, and sometimes this can change what you previously had established. Items and information you had previously deemed "private," (again, nothing is truly private), may become more publically available as these privacy settings and policies change. Make a habit of frequently checking, reviewing, and educating yourself on the latest privacy updates so you know exactly how and where your information is available on Facebook.

Facebook groups have also become an issue. Facebook offers users the opportunity to create closed, and seemingly "private" groups where users with similar interests can come together to communicate and share information. Just like with your personal profile, these groups are far from truly secure. Any group member can take screen shots and share information you have posted. Even if you are a passive member and do not post to the group, as a member of the group you can be held accountable for the group's actions, views, and expressions. For example, if you are a member of a political group on Facebook, you can be held accountable for the political views stated and shared by the group.

Twitter

Twitter is a popular, text-based sharing platform. Users may post up to 280 characters, with photos or videos attached, to their personal profile. They can also "re-tweet," or re-post, and "like" things shared by other users. While you may not have been the originator of a post, you are still responsible for anything you share or "re-tweet." Sharing or liking another tweet can be viewed as an agreement or acceptance of the views expressed in it. For example, while your personal tweets may be "private" and only available to your followers, if you like a tweet from a political figure, that can be read as political activity.

Twitter may feel like a more casual platform, and thus a more acceptable place to relax your guard and share things otherwise deemed inappropriate, but it is for this reason that users should be apprehensive and diligent when using the platform.

Instagram

Instagram is a mobile photo-sharing app. Instagram is more limited than other platforms in the type of information that can be shared, but photos are often the easiest and most revealing information someone can share. Like other platforms, Instagram photos that are seemingly private can be screenshot and shared by whoever has the file, despite assumed privacy settings.

Accounts that are not private can also have their photos pushed into the "videos and photos you may like" sections of other users, as part of Instagram's larger algorithm, which uses hashtags, interests, and locations to find and pull photos to present to other users. If your account isn't private, your photos are subject to this.

Snapchat

Snapchat is a mobile photo and video sharing app that allows people to post photos, videos, and send messages that last for a limited amount of time. Following a predetermined amount of time, from a few seconds to 24 hours, the content seemingly "disappears." However, while you may not be able to access it, Snapchat retains the files. These photos, videos and messages are no longer your property, a fact you should consider when using the app.

Like other platforms, Snapchat content can also be screenshot, though it typically alerts the content originator when this happens. Those screenshot files are then out of your control and can be shared and disseminated without your knowledge. This can create a false sense of security. You may forget that you sent specific content, or think that it has "disappeared" through Snapchat's timer function, while it may very well still exist in a photo file on someone else's device.

Dating Apps

In 2017, many people use dating apps such as Tinder, Bumble, Plenty of Fish, OkCupid, and Zoosk to find and pursue romantic partners. Marines are not prohibited from using these apps, but they should be aware that they pose the same risks as every other social media platform available to them. Identifying yourself as a Marine on these sites can open yourself up as a target to an audience of people you don't know.

Your actions still represent I MEF and the Marine Corps, something you should consider when sharing photos and information about yourself with an audience that is comprised completely of strangers. Treat everyone with dignity and respect, because you are always a representative of I MEF and the Marine Corps in every action, both online and in person. Dating apps are notorious for inappropriate and embarrassing interactions. Just like other platforms, dating apps are subject to screenshots. Anyone can take a photo of your content and share it as they see fit. Avoid these at all costs by adhering to the standards of decency and respect expected of you as a member of I MEF.

Initial Steps

The following are some basic and initial steps you can take to guard yourself and your family online.

Profile Information/Status Updates

- Keep sensitive, work-related information off your profile.
- Keep your plans, schedules and location data to yourself.
- Protect the names and information of coworkers, friends and family members.
- Adhere to the Uniform Code of Military Justice and other applicable policies.

Posted Data

- Check all photos for potential violations of operational security, including reflective surfaces.
- Check filenames and file tags for sensitive data (names, organizations, etc).

- Remove geotagging information from your posted content.
- Tell friends to be careful when posting photos and information about you and your family.
- Let subject matter experts respond to negative posts. You may come across negative or disparaging posts about the Marine Corps or see third parties initiating negative conversations. Unless you are a trained Marine Corps online spokesperson operating in an official capacity, avoid the temptation to react yourself.

Settings and Privacy

- Carefully look for and set all your privacy and security options on every platform you utilize.
- Determine both your profile and search visibility.
- Sort "friends" into groups and networks and set access permissions accordingly.
- Verify through other channels that a "friend" request was actually from your friend.
- Do not accept a friend request unless it is from someone you know.

Security

- Keep your anti-virus software updated.
- Beware of links, downloads and attachments just as you would in emails.
- Beware of apps or plugins that are written by unknown third parties to access your data.
- Look for "HTTPS" in the address bar and the lock icon that indicates active transmission security before logging into a website or entering sensitive data.
- Avoid posting photos or videos with "geotags." These release your exact location at the time of posting and can be detrimental to operational security. Be wary of "check-in" functions and mobile apps requests to access your location.

Passwords

- Use unique passwords for each online site you use.
- Ensure your passwords are sufficiently hard to guess.
- Do not share your passwords with anyone.
- Update your passwords regularly and keep them complex. Include multiple special characters (!@#$), numbers, and upper and lowercase letters.