FORWARD

Capt. Tony Hahn
Chief, Office of Public Affairs

Social media has advanced our ability to tell the Coast Guard’s story and has uniquely allowed us to engage in direct dialogue with our audience. This unique relationship has forged an incredible group that in turn tells our story for us and advocates for us as our “Brand Ambassadors.”

To build and enhance this relationship, we must continue to leverage new opportunities, social media platforms and expand our audience. This is a fast paced, very dynamic communications environment that will need a deliberate and unified approach. Our social media guide is a living document that we update frequently to ensure everyone in the Coast Guard understands our strategy, how to employ our social media tools optimally, and how we all must use social media in a responsible, safe, and effective manner.

Social media provides us an amazing opportunity to reach audiences that we have never been able to reach and your personal use of social media can be a big part of this. As Coast Guard men and women, we must always remember we represent the service at all times and this guide provides key information that illuminates how this critically applies to your use of social media.

If you see something in the guide that doesn’t answer your questions, please feel free to contact my Chief of Social Media, Lt. Jodie Knox, or me. I sincerely appreciate all the hard work you do everyday telling our story.

Semper Paratus

TH
# Table of Contents

1. **RIGHT TOOL, RIGHT LEVEL, RIGHT AUDIENCE**
   - Strategy ............................................ 1
   - Social media toolkit ............................. 1
   - Engagement ..................................... 2
   - Way ahead ..................................... 2

2. **PERSONAL USE** ................................. 3
   - Official, unofficial or personal ............. 3
   - Reputation ..................................... 3
   - Privacy ......................................... 4
   - Responsibility checklist .................... 5

3. **PROFESSIONAL USE** ......................... 6
   - Manage ......................................... 6
   - Policy ......................................... 6
   - Establishing a social media presence ...... 9
   - Official post checklist ....................... 10
   - Operational security for official pages checklist .... 11

4. **FAMILY USE** .................................. 13
   - Support ....................................... 13
   - Family guide .................................. 13
   - Privacy protection checklist ............... 14

5. **ACCOUNT SAFETY & SECURITY** ........... 15
   - Awareness .................................... 15
   - Account Safety & Security checklist ....... 16

6. **REFERENCES** .................................. 18
   - Facebook quick reference guide .......... 18
   - Twitter quick reference guide ............. 19
   - Frequently asked questions ............... 20
   - Official social media sites ................. 22
Over the past several years the U.S. Coast Guard has been engaged in social media as it’s evolved from one initially dominated by MySpace, revolutionized by blogs and bloggers and subsequently transformed by Facebook.

**Strategy**

The Coast Guard Commandant’s vision for social media guides our strategy. Our social media program complements our existing public affairs efforts as part of a comprehensive communication plan to educate and engage the public. We will utilize best practices to deploy the right tool, at the right level, for the right audience.

The emergence of Facebook as the dominant social media networking site is fortuitous as it affords us the opportunity to communicate our message in words, pictures and video to target audiences we might not otherwise reach through traditional media outlets. As stories progress from the unit to national level, the rest of the social media toolkit will maximize our exposure to most efficiently allocate public affairs resources.

**Social Media Toolkit**

As public affairs professionals, we rely on three basic mediums to tell the Coast Guard story: words, pictures and video. The social media landscape allows us to take advantage of these core strengths to directly communicate our information utilizing the following social media toolkit:

- **Word Press:** WordPress is the blog content management system (CMS) of choice for nearly 13 million bloggers – including the DoD, where Coast Guard blogs are hosted. The Coast Guard uses blogs at the district and national levels to communicate our messages to niche audiences, policy makers and the public.

- **Facebook:** Facebook.com is the second most visited website destination in America following google.com. As America’s fastest-growing one-stop social media destination with 890 million daily active users, Facebook serves as the centerpiece of our social media efforts from Coast Guard units to the national level.

- **Twitter:** Twitter allows in excess of 65 million Americans to communicate in real time via micro blogs of 140 characters or less. While Twitter tends to be limited by topical trends, it can be an effective means of communicating with media and niche audiences if properly managed.
♦ Youtube: The most popular video sharing site in the world, YouTube has an audience of more than 1 billion active users each month. In conjunction with DVIDS, it is an effective means of getting the Coast Guard story out through multimedia products.

♦ Instagram: Instagram has become an immensely popular tool for sharing photos and short video clips. Instagram serves as a means to give the American public a “day-in-the-life” view of Coast Guard units across the service by enabling various units to guest host and post daily photos of missions and operations. Instagram has more than 300 million active users.

♦ Flickr: Flickr is the lead photo management and sharing application for showcasing the best Coast Guard imagery. It allows anyone to download high-resolution imagery of Coast Guard missions, operations and people.

Engagement

The permeation of online social media tools into the standard communication toolkit presents Coast Guard communicators with access to and the opportunity to engage an ever-growing and influential new audience. Using online tools such as PIER, we can push messages and stories to the approximately 150 million + Americans (nearly half the population) who get at least some of their news from online sources.

While push tools such as PIER are effective, we gain substantial outcomes through social media tools as they afford us the opportunity for direct two-way engagement with the American people which allows us to “listen” to our constituencies and consider both their feedback and criticisms of how we do business as part of our larger organizational growth process. This engagement is at the core of our social media strategy and, in many ways, is its very reason for being.

As one of the five Armed Services, the Coast Guard is very unique. We are defenders of the homeland, but also a federal regulatory agency. As a result, we rely on mass communications tools to not only broadcast our messages but to seek input from those our rules and policies govern. The Coast Guard is headquartered in Washington, D.C., but the service is made up of hundreds of independent commands in communities across the country, and in many instances around the world. As a result, our communications efforts are localized and our commanders rely on both the good will and the first hand experience of those who call the community home to be effective partners in mission execution.

The biggest challenge moving forward is the dynamic rate at which social media tools and tactics change. Our strategy, therefore, must account for an ever changing online environment and the rise and fall of social networks both in size and efficacy.

The Way Ahead

After several years of development and use, the Coast Guard’s social media program has adopted a communication strategy based on best practices and guided by the Commandant of the Coast Guard’s vision. This evolution of the social media program is a testament to our leadership and their embrace of social media as a communication tool.

Following the principles of Right Tool, Right Level, Right Audience, the Coast Guard has centralized and focused our use of social media tools to complement our media relations program and maximize our impact with unique audiences.
While Coast Guard personnel are the best people to tell the Coast Guard story, they must engage online responsibly. Personnel who use social media should share information with the understanding and realization that nothing posted online is truly private.

Coast Guard members must responsibly engage in unofficial social media posting about the Coast Guard and topics related to our service. Any content that you personally post on any Internet site is considered “unofficial.”

**Official, Unofficial or Personal**

1. **Official**: Engaging on social media IS your job and you are doing it on behalf of the Coast Guard.

2. **Unofficial**: Engaging on social media IS RELATED to your job, but you are doing so in a personal capacity. What you are posting online mentions the Coast Guard, your job or your experience.

3. **Personal**: Engaging on social media IS NOT RELATED to your job. What you are posting does NOT mention the Coast Guard in any way.

**Reputation**

We must be vigilant, sensible and disciplined so our actions online do not jeopardize our public reputation, interfere with Coast Guard missions or discredit the service. This guidance applies to anything said, written, posted or shared on the Internet, including personal comments, photos, videos or graphics, blogs, forums, wikis, multimedia sharing sites or any other Internet site or application.

You are encouraged to professionally and respectfully correct errors and misrepresentations, made by others, about the Coast Guard. However, remember to respond and act with your perspective, not your emotions, when posting content. Refer to your chain of command or servicing public affairs office for guidance if you're uncertain about the appropriateness of a response. If you decide to identify yourself as a Coast Guard member, don't disguise, impersonate or otherwise misrepresent your identity or affiliation with the Coast Guard. Stating your rank or grade, occupation and status (active, reserve, civilian, auxiliary) is acceptable as well.

Do not self promote or accept payments. Using your job, rank or responsibilities to promote yourself online and accepting compensation for writing about your official connection with the service is not authorized. Treat requests for postings that relate to a current or former Coast Guard job or responsibility as a media request.
Privacy

Social media users should be vigilant in protecting their privacy and the privacy of others online. You should never assume confidentiality online regardless of how strict your privacy settings are. We must ensure that we, our families and loved ones keep themselves safe and do not compromise the safety and security of Coast Guard members and operations. Providing too much information about your private life, your home life or daily routine can provide details that can be used maliciously. Be careful to protect yourself and your privacy.

The best way to protect your privacy and prevent Internet-related crimes, like identity theft, on social media sites is by maintaining your privacy settings. Posting or disclosing internal Coast Guard documents or information that the Coast Guard has not officially released to the public is prohibited — period.
PERSONAL USE

RESPONSIBILITY CHECKLIST

☐ Obey the law: Do not violate intellectual property rights including copyright protections. Do not use U.S. Coast Guard protected words or symbols without prior authorization.

☐ Be responsible: Anything you post on the web including text and pictures can easily be shared, taken out of context or used maliciously.

☐ Online doesn’t mean anonymous: There is no such thing as anonymity online. Even if you decide not to fully identify yourself, you should not disguise, impersonate or otherwise misrepresent who you are and your association with the Coast Guard.

☐ Practice restraint: Be respectful, accurate and professional. Always use your best judgement and consider how the content reflects upon yourself, your unit and the U.S. Coast Guard.

☐ Are you talking about the Coast Guard? Comment carefully. Stay in your lane and only talk about what you know, your personal experiences and professional expertise. You may use your name, rank and position to disclose your affiliation with the service. Do not forget OPSEC!
The following guidelines are for members and employees who engage on social media sites in their official duties. In other words, what you are posting online is on behalf of a Coast Guard unit, command or other entity.

When you are assigned as a public affairs officer or the social media site manager, everything you do impacts public trust. You are a direct representative of the Coast Guard and must embody the spirit and professionalism of the service.

Social media is a powerful communication tool. When used correctly, it can help the Coast Guard reach a wide audience. Social media can be used to help engage in the conversation while at the same time promote awareness of our service’s communication priorities. Using social media effectively is a process: social media should be an extension of, not a substitute for, an official government website.

**Manage**

Regardless of how you were chosen, what your background is or even how much you know about the field of social media, everyone who represents the Coast Guard in social communication has a unique opportunity to engage in potentially thousands of online conversations about the Coast Guard every day. It is a great opportunity and puts you at the forefront of telling the Coast Guard’s story.

With the assignment to manage and conduct social media on behalf of the Coast Guard, you must remember: everything you do balances on public trust — this is the foundation upon which the success of public affairs and social media is built.

As part of your duties, you will actively engage the public, ensuring that you consider and promote unity of voice, freedom of information, timeliness, and accuracy while maintaining security and privacy.

**Establishing a presence**

1. Determine what you plan to achieve with your social media presence. Make sure you have a way forward and a set of goals. Developing a social media outreach plan requires a lot of thought, so make sure you know how you plan to use social media to communicate.

2. Review all applicable public affairs policy. This handbook is a great start, but there are more materials at your disposal, including the External Affairs Manual and External Affairs Tactics, Techniques and Procedures.

3. After you’ve completed the basic research, work with your command to develop a social media strategy as part of your unit’s larger communication strategy. The Coast Guard has a strategy for each
social media platform. This helps your organization refine its focus. During this phase of the planning process, it’s also helpful to look at how other units are using social media.

4. Once you’ve done your research and you’re confident in setting up a social media presence, you will need to request a presence through your servicing public affairs office.

5. Registering social media sites is required. All official Coast Guard social media sites must be registered with Commandant (CG-0922). A link to the registration form is located on the Coast Guard Compass blog (http://coastguard.dodlive.mil) under the “Official Sites” link. Commands shall update their registration if their designated social media spokesperson changes.

6. Once you’re up and running, the process isn’t over. Make sure you post often and keep your social media presence active. A stagnant social media presence is an ineffective social media presence.
**PROFESSIONAL USE**

**ESTABLISHING A SOCIAL MEDIA PRESENCE**

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receive Command Approval</td>
<td></td>
</tr>
<tr>
<td>Review Policies and Resource Material</td>
<td></td>
</tr>
<tr>
<td>Determine Your Goals</td>
<td></td>
</tr>
<tr>
<td>Determine Your Audience</td>
<td></td>
</tr>
<tr>
<td>Identify Appropriate Social Media Platforms</td>
<td></td>
</tr>
<tr>
<td>Draft Content Strategy</td>
<td></td>
</tr>
<tr>
<td>Determine Site Management Strategy</td>
<td></td>
</tr>
<tr>
<td>Post Disclaimer Text</td>
<td></td>
</tr>
<tr>
<td>Clearly Identify Site as “Official”</td>
<td></td>
</tr>
</tbody>
</table>
PROFESSIONAL USE

OFFICIAL POSTS CHECKLIST

☐ Post Relevant Content: Develop a content management plan to guide postings & ensure what is posted interests your audience. Be unique and use your insider access to take the reader behind the scenes of your job.

☐ Comply with policy: Have a method in place to ensure there is a thorough content review before posting (SAPP) conduct a security review, and ensure command approval.

☐ Ensure content is accessible to all audiences: Content should comply with Section 508 requirements. Include closed captioning and/or transcript files on videos and alt text on imagery/graphics.

☐ Moderate comments: Post the official comment policy and moderate comments on the site accordingly. Engage when needed.

☐ Stay in your lane: Do not comment on what you do not know. Direct inquiries to appropriate POC.

☐ Keep records: Keep records of your online interactions and conversations.

☐ Provide appropriate attribution: Links to unofficial content, such as news articles or multimedia, are authorized as long as proper credit is given to the source.
OPERATIONAL SECURITY FOR OFFICIAL PAGES

☐ Make sure all members posting to official sites are current on OPSEC training.

☐ Content is submitted and approved by release authority prior to posting.

☐ Content is published in accordance with public affairs guidance.

☐ Monitor posts to ensure users are not commenting or posting sensitive information.

☐ Conduct regular social media OPSEC training within your team and with your units.

☐ Inform members and their families on the importance of operational security in a social media environment.

☐ Be vigilant. Never become complacent when it comes to OPSEC. Always check for violations. Once the information is out there, you can’t take it back.
Family Use

The primary purpose of establishing a social media program is to communicate with the public and highlight the Coast Guard’s roles and missions. As a secondary benefit, commands can leverage social media to help keep families and the Coast Guard connected.

Support

Coast Guard men and women could not perform their missions without the support and concern of family members and the military community.

When units communicate with families, they should never assume confidentiality online regardless of how strict your privacy settings are. We must keep ourselves and our families safe and not compromise the safety and security of Coast Guard members and operations.

Facebook brings command information to the family through a medium that they already use – which is why it works so well. The trouble is, others can gain access to this same content – all in one place too. Those “others” aren’t looking to join in the discussion, though they are looking for ways to steal your identity, use the information to infiltrate government networks or conduct other forms of illegal or dangerous actions.

Facebook is not considered a family readiness tool for unit personnel. The platform is a good way to communicate and hold open discussions, but is far too open a forum to share and discuss specific details, such as who they are, who their family members are, when and where a unit will be pulling into port, when Coast Guard members are returning from deployment, etc.

This platform is, however, one you can leverage for outreach to community members, family and friends.
FAMILY USE

PRIVACY PROTECTION CHECKLIST

☐ Never accept the “default” settings for sites. Personally go through your settings and select the appropriate level of protection for you, your family and the Coast Guard.

☐ Don’t share details about yourself, your family members or others online including social security numbers, birthdates, contact information, home addresses, details about lifestyles or careers, and any other personally identifiable information.

☐ Cautiously use location-based social networking, as this provides specific details about your daily habits to the public including adversaries.

☐ Do not “friend” or grant access to people you do not know and trust.

☐ Be aware that nothing is really ever private online. What is posted on the web can easily be shared, taken out of context or used maliciously.

☐ Use strong passwords to protect your accounts. It is suggested to have 14+ characters including a combination of upper and lower case letters, numbers and symbols.
Account Safety & Security

Awareness

Using social media on a daily basis to tell the Coast Guard’s story makes us more susceptible to cyber attacks and threats, such as hacking or an account being otherwise compromised. In order to keep official accounts secure, we must remain vigilant and take necessary precautions to limit access to these accounts from unauthorized users. Some of these same steps can be taken to ensure your personal accounts stay safe as well.

All official accounts should be linked to an official uscg.mil email address. Utilizing official email addresses ensures that recovery information can be obtained – even if you become unable to access your personal email for some reason.

Passwords should be changed regularly and never be shared publically. A strong password must consist of a combination of upper and lowercase letters, special characters and numbers. Passwords should be changed monthly and no two accounts should have the same password. Regularly review who has access to official accounts and ensure passwords are changed during transfer season after any administrators depart.

Often times, social media sites offer two-step verification for signing in. The accounts should be linked to a government issued cell phone for added security. Enabling two-step verification, when possible, is a crucial step in ensuring accounts cannot become compromised.

Facebook forces you to be logged into your personal account to access the official Coast Guard account. If you administer one of these accounts, your personal account should be kept secure with the same guidelines above.

Recently, terrorists and other radical extremist groups have utilized social media platforms to communicate, recruit, and in some instances, make threats. Any concerning engagement along these lines should immediately be reported to your Command Center for proper documentation and investigation.

Be aware of the possibility of imposter accounts. Inform CG-0922 if you suspect an account may be compromised.

If you have any questions or need additional guidance on account security or what to do if an account becomes compromised, contact CG-0922 via email at socialmedia@uscg.mil.
COAST GUARD

SAFETY & SECURITY CHECKLIST

☐ Ensure passwords are changed regularly using a combination of upper and lowercase letters, numbers and special characters.

☐ If supported by the social media platform, enable two-step verification for account login. Ensure all official accounts are linked to government email addresses and your unit’s duty cell phone number.

☐ When a social media platform links to your personal account (e.g. Facebook), ensure the same account security tips listed above are followed.

☐ In any instance of a safety or security issue, such as a hack, threat or compromise, immediately contact CG-09222 for reporting to the appropriate platform manager.

☐ Report any instances of hacking, terrorist-related comments, threats, compromised accounts or any other concerning engagement to your Command Center.
Facebook: Quick Reference Guide

1. Tag other pages when possible or appropriate.
2. Ask engaging questions.
3. Respond to questions in a timely manner.
4. Post in a conversational tone.
5. Spellcheck and review every post prior to posting.
6. Thank followers and praise them often.
7. Include compelling imagery in every post (photos, graphics or videos.)
8. Welcome participation, collaboration and feedback.
9. Use URL shorteners.
10. “Like” sister organizations and tag them often.
11. Utilize subject matter experts to respond to questions you’re unfamiliar with.
12. Avoid automated posting services for posting to multiple sites.
13. Don’t over post or under post. The frequency will depend on your audience size.
14. Do not cut and paste news releases.
15. Don’t “delete” comments, “hide” them (review NARA regulations).
16. Track metrics and evaluate how content performs.
17. Always be mindful of OPSEC when posting!
18. It can take only one slip up to discredit our reputation!
Twitter: Quick Reference Guide

1. Use approved URL shorteners.
2. Use unique hashtags for specific events or initiatives.
3. Spellcheck and review every tweet prior to posting.
4. Utilize Twitter to communicate before, during and after a crisis.
5. If retweeting content, try to add in Coast Guard messages when appropriate.
6. Engage your audience by asking questions, then retweet the answer.
7. Check direct messages and mentions daily. Then respond.
8. Keep continuity with the voice of your unit when different members tweet.
9. Become the go-to source of information.
10. Use direct messages to engage with audience.
11. Utilize subject matter experts to respond to questions you’re unfamiliar with.
12. Avoid automated posting services for posting to multiple sites.
13. Don’t over tweet or under tweet. The frequency will depend on your audience size.
14. Do not follow brands (Coke, Nike).
15. Use twitter language, but keep it professional.
16. Track metrics and evaluate how content performs.
17. Always be mindful of OPSEC when tweeting!
18. It can take only one slip up to discredit our reputation!
Frequently Asked Questions

Q: How do I get content on the Coast Guard’s national social media sites?
A: E-mail stories, photos or links to your servicing public affairs office. You may also contact the Coast Guard Social Media team (CG-0922) at: socialmedia@uscg.mil. We will work hard to feature your content on our sites based on our editorial calendar.

Q: Who is allowed to manage my unit’s Facebook page?
A: Public affairs specialists usually take the role as social media managers since content posted on these sites is often times news or operational information. But you don’t have to be a PA to become a social media manager. With command approval any Coast Guardsman can run a social media site as long as they work closely with their unit’s servicing public affairs office and have received social media training.

Q: Can I delete comments on my unit’s Facebook page?
A: Every registered social media presence in the Coast Guard is required to have a posting policy that indicates what can and cannot be posted to Facebook pages. If users violate these terms you are entitled to hide the comment. But be mindful that Facebook is about facilitating a conversation, so stick to the posting policy. Don’t remove or hide comments just because they express negative opinions about the organization.

Q: How can I increase the number of followers on Facebook or Twitter?
A: Be creative. There is no surefire way to increase followers. Engage your audience as much as possible and never leave accounts stagnate. Become the go-to source for information. If another unit is having success with a campaign or are engaging their audience in a unique way, feel free to emulate that. Appropriate social media trends (i.e. Throwback Thursday), can be a good way to engage and increase followership. However, any social media trend should be appropriate and reflect positively upon our service. Remember that you are representing the Coast Guard and no inappropriate jokes, comments, pranks or other unprofessional trends should be shared.
Q: What happens if someone is impersonating me or someone in my unit?
A: Contact CG-0922 for assistance.

Q: Where should I direct recruiting questions?
A: Refer them to the Coast Guard recruiting website www.gocoastguard.com.

Q: A family member posted something that violates OPSEC? What do I do?
A: Take a screenshot of the post, immediately remove or hide the post (if possible) and then route the screenshot and any details to your command center for their awareness. Next, engage that person and explain why the type of information isn’t appropriate for conversation online. You must notify your command so that they are informed of the OPSEC breach and can take appropriate action.

Q: What should I do if I find an unofficial social media page created by a family member or command?
A: Many commands have unofficial social media presences established by veterans or fans of our service. We do not have the right to remove these presences nor would we want to unless they portrayed themselves as an official presence or are using protected words or symbols. In the meantime, work with command leadership to determine if you want to approach the page and/or simply monitor it and chime in when you have information to add. You may also want to contact the administrator to touch base.

Q: I’m transferring my duties as the social media manager. What should I do?
A: If you established your social media presences under a general command account, it is as simple as turning over the login and passwords and teaching the new social media manager how the platform works. Make sure to give the new social media manager administrator privileges. Alert your servicing district public affairs office and alert CG-0922.
Coast Guard Social Media Websites

coastguard.dodlive.mil
allhands.coastguard.dodlive.mil
mariners.coastguard.dodlive.mil

www.facebook.com/UScoastguard

www.youtube.com/USCGImagery

www.twitter.com/USCG

www.flickr.com/photos/coast_guard/

instagram.com/uscg