NAVY

SOCIAL MEDIA HANDBOOK

AUGUST 2018

Navy Office of Information
www.navy.mil/socialmedia
navysocialmedia@navy.mil
703-614-9154

AMERICA'S NAVY
FORGED BY THE SEA

U.S. Navy Social Media Handbook

for Navy leaders, communicators, Sailors, families, ombudsmen and civilians

August 2018

This handbook is an update of the January 2018 handbook.
It reflects a change in the link to report tips to NCIS.
No other changes were made.

INTRODUCTION

Social media continues to revolutionize our lives, from the way we communicate and interact with the world to the content we see and the news we read. As a result, the way people get information has drastically changed, and the desire to have real-time conversations with individuals, organizations and government entities has increased. This presents a tremendous opportunity for everyone, from Sailors and families to Navy leaders and ombudsmen, to more effectively communicate with one another and to share the Navy story more broadly.

The proper and effective use of social media presents unequaled opportunities for you to share our Navy's story in an authentic, transparent and rapid manner while building richer, 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 new challenges, operational and cybersecurity considerations as well as concerns regarding online conduct. New decisions on which platforms are best to use ensure the most relevant information is conveyed are being deliberate in real-time as platforms rapidly adapt, age-out or emerge. This handbook's sections are tailored to the unique audience it's serving: Navy leaders, communicators, Sailors, families, ombudsmen and civilians.

Since social media is constantly evolving, we've included only enduring information that will remain relevant. We encourage you to frequently visit *http://www.navy.mil/socialmedia* for the latest policy, guidelines, best practices, standard operating procedures, training and other resources.

If you have questions or want to share feedback, contact the Navy Office of Information at 703-614-9154 or *navysocialmedia@navy.mil*.

CONTENTS

LEADERS 2

Overview of Today's Online Landscape 2
Unofficial (Personal) Use of Social Media 3
Setting the Standard for Online Conduct 3
Reporting Incidents 4
Operations Security (OPSEC) 4
Politics 5
Endorsements 5
Impersonators 5

NAVY COMMUNICATORS 6

Overview of Today's Online Landscape 7
Official Use of Social Media for Navy Commands 7
Policy 8
Deciding if Social Media is Right for a Command 9
Alternatives 9
Strategy Development 9
Content Planning 10
Crisis Communication: Casualties and Adverse Incidents 12
Account Security 17
Operations Security (OPSEC) 18
Politics and Endorsements 18
Online Advertising 19
Online Conduct 19
Impersonators 19

SAILORS 20

Online Conduct 20
Follow the UCMJ 20
Reporting Incidents 21
Politics 21
Cybersecurity 21
Operations Security (OPSEC) 21
Adverse Incidents 22
Endorsements 22

FAMILIES 23

Cybersecurity 23
Operations Security (OPSEC) 23
Adverse Incidents 24

OMBUDSMEN 25

Overview of Today's Landscape 25
Best Practices to Support Command's Official Social Media Presence(s) 25
Cybersecurity 26
Operations Security (OPSEC) 26
Adverse Incidents 27
Private Groups 27

DEPARTMENT OF THE NAVY CIVILIANS 28

Cybersecurity 28
Operations Security (OPSEC) 28
Online Conduct 28
Politics 29

APPENDIX 30

Online Conduct 30
Joining Networks 30
Setting Guidelines 30
The UCMJ and Navy Regulations 30
Behaviors with Legal Consequences 31
Reporting Incidents 31
Bottom Line 31
Online Safety and Best Practices 32
Security 33

LEADERS

The Navy has an obligation to provide timely and accurate information to the public, keep our Sailors and Department of the Navy civilians as well as their families informed, and build relationships with our communities. As a Navy leader, you are a crucial part of those communication efforts.

Social media presents unequaled opportunities for you to share the Navy story in an authentic, transparent and rapid manner while building richer, more substantive relationships with people you may not have reached through traditional communication channels. It is important to remember that the effective use of social media is only part of a command's public affairs program. Navy leaders need to work with their public affairs team to decide whether social media is appropriate for their command; not every command needs to use social media. Conversations about the Navy will still take place on social media; however, they will not include the Navy's perspective.

This handbook will teach you the best practices that you should follow while communicating about the Navy on social media.

Overview of Today's Online Landscape

Social media usage is nearly universal among younger adults and is quickly growing among people over age 50. People use it to consume news, make or strengthen connections, and engage in discussions and activism related to personal interests. There are many different social media platforms, each with distinct use cases. Navy leaders need to work with their public affairs team to focus their efforts on a social media platform that aligns with the command's communications objectives and that its targeted audiences use regularly.

According to a study conducted in 2016 by Pew Research Center, the percentage of adults who use at least one social media site is as follows: 82 percent of 18-29 year olds, 77 percent of 30-49 year olds, 65 percent of 50-64 year olds, and 35 percent of people age 65 and above. In total, nearly 70 percent of adults use social media. Specifically, 68 percent use Facebook, 25 percent use Instagram and 21 percent use Twitter. Of the 68 percent of adults using Facebook, over 75 percent go onto the platform every day. Fewer users reported logging onto Instagram (51 percent) and Twitter (42 percent) daily.

The majority of Facebook users (66 percent) say they mostly friend or follow people they know personally on Facebook. They don't necessarily log onto it for news; 62 percent of users say they see it on Facebook while doing other things. Conversely, 54 percent of Twitter users say they're looking for news on Twitter. Only 15 percent of Twitter users reported that they normally follow people they know personally, whereas 48 percent say they mostly follow people they don't know personally.

Unofficial (Personal) Use of Social Media

Unofficial internet posts are posts published on any internet site by a Sailor or a Department of the Navy civilian in an unofficial, personal capacity that include content about and/or related to the Navy or Sailors.

The term "posts" includes, but is not limited to, personal comments, blogs, photographs, videos and graphics. The term "internet sites" includes, but is not limited to, social networking platforms, messaging apps, photo- and video-sharing apps and sites, blogs, forums and websites with comment sections.

If you are expressing a personal opinion of any kind, it is your responsibility to make clear that you are not speaking for the Navy and that the stance is your own and not representative of the views of the Navy.

Setting the Standard for Online Conduct

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

If evidence of a violation of command policy, Uniform Code of Military Justice 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 Navy regulations, you have an affirmative obligation to act upon offenses under the UCMJ which come under your observation. This adds an ethical wrinkle to friending or following your subordinates; the key is for you to maintain the same relationship with them at work as you do online and to be clear about that.

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

Punitive action may include Articles 88, 89, 91, 92, 120b, 120c, 133 or 134 (General Article provisions, Contempt, Disrespect, Insubordination, Indecent Language, Communicating a threat, Solicitation to commit another Offense, and Child Pornography offenses), as well as other articles, including Navy Regulations Article 1168, nonconsensual distribution or broadcast of an intimate image.

Behaviors with legal consequences include:

- Child exploitation/Child sexual exploitation
- Computer misuse ("hacking")
- Cyber stalking
- Electronic harassment
- Electronic threats
- Obscenity

Consult your command's JAG for legal counsel.

Reporting Incidents

Any member of the Navy community who experiences or witnesses incidents of improper online behavior should promptly report it to their chain of command via the Command Managed Equal Opportunity manager or Fleet and Family Support office. Additional avenues for reporting include Equal Employment Opportunity offices, the Inspector General, Sexual Assault Prevention and Response offices and 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.

Specific instructions are available at *http://www.ncis.navy.mil/pages/NCISTips.aspx*.

Refer to the handbook's *appendix* for additional information.

Operations Security (OPSEC)

One of the best features of social media platforms is the ability to connect people from across the world in spontaneous and interactive ways. Like most things that we do as a Navy, social media can present risks and challenges such as OPSEC, but they can be mitigated. Embrace the risks and challenges by reinforcing OPSEC rules, which are universal and should be maintained online just as they are offline. Make sure your Sailors and Navy civilians as well as their families know that if they wouldn't say it, write it or type it, they shouldn't post it on the internet.

OPSEC violations commonly occur when personnel share information with people they do not know well or if their social media accounts have loose privacy settings. As a Navy leader, carefully consider the level of detail used when posting information anywhere on the internet. Reinforce OPSEC best practices such as limiting the information that your Sailors, Navy civilians and families post about themselves, including names, addresses, birth dates, birthplace, local towns, schools, etc. Work with your public affairs team to ensure best practices and standard operating procedures, addressed in this handbook's section for Navy communicators, are implemented.

Politics

Sailors 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 Sailors 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 their own and not those of the U.S. Navy or Department of Defense.

Sailors may not engage in any partisan political activity – such as posting direct links to a political party, campaign, group or cause on social media, which 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.

Department of the Navy civilians need to consider the Hatch Act and DoD policy, which are both addressed on *page 29*.

Endorsements

Navy leaders must not officially endorse or appear to endorse any non-Federal entity, event, product, service or enterprise, including membership drives for organizations and fundraising activities. No Sailor may solicit gifts or prizes for command events in any capacity – on duty, off duty or in a personal capacity.

Impersonators

Impostor accounts violate most social media platforms' terms of service agreements.

The best offense is a good defense. Regularly search for impostors and report them to the social media site.

The impersonation of a senior Navy official, such as a flag officer or a commanding officer, should also be reported to the Navy Office of Information at 703-614-9154 and *navysocialmedia@navy.mil*.

NAVY COMMUNICATORS

The Navy has an obligation to provide timely and accurate information to the public, keep our Sailors and Department of the Navy civilians as well as their families informed, and build relationships with our communities.

Social media presents unequaled opportunities for you to share our Navy's story in an authentic, transparent and rapid manner while building richer, more substantive relationships with people you may not have reached through traditional communication channels. It is important to remember that the effective use of social media is only part of a command's public affairs program. Navy communicators need to work with their command leadership to decide whether social media is appropriate for their command; not every command needs to use social media.

Additionally, social media has led to new, creative ways and places to quickly and directly tell your command's story. Your content – stories, photos, videos (b-roll and productions), infographics (still and video), blogs, etc. – is needed to tell our Navy's story. Submit released stories to the Navy.mil content management system and Navy Live blog proposals to *navysocialmedia@navy.mil*. Follow current instructions on visual information release and records management. Forward released imagery of significant importance to CHINFO Navy Media Content Operations for wider distribution and archiving.

Refer to http://imagery.navy.mil for content submission SOPs.

Finally, while this handbook will teach you best practices to tell our Navy's story on social media, remember that there is no substitute for personally using social media to understand how to use it professionally.

Overview of Today's Online Landscape

Social media usage is nearly universal among younger adults and is quickly growing among people over age 50. People use it to consume news, make or strengthen connections, and engage in discussions and activism related to personal interests. There are many different social media platforms, each with distinct use cases. As a Navy communicator, you need to focus your efforts on a social media platform that aligns with your command's communications objectives and that your targeted audiences use regularly.

According to a study conducted in 2016 by Pew Research Center, the percentage of adults who use at least one social media site is as follows: 82 percent of 18-29 year olds, 77 percent of 30-49 year olds, 65 percent of 50-64 year olds, and 35 percent of people age 65 and above. In total, nearly 70 percent of adults use social media. Specifically, 68 percent use Facebook, 25 percent use Instagram and 21 percent use Twitter. Of the 68 percent of adults using Facebook, over 75 percent go onto the platform every day. Fewer users reported logging onto Instagram (51 percent) and Twitter (42 percent) daily.

The majority of Facebook users (66 percent) say they mostly friend or follow people they know personally on Facebook. They don't necessarily log onto it for news; 62 percent of users say they see it on Facebook while doing other things. Conversely, 54 percent of Twitter users say they're looking for news on Twitter. Only 15 percent of Twitter users reported that they normally follow people they know personally, whereas 48 percent say they mostly follow people they don't know personally.

We know that young people are very active on social media, but they are less likely to show they are engaged in content. Though people age 18-29 are almost 20 percent more likely to use social media than people age 50-64, the older group is 4 percent more likely to share or repost a news story on social media and 10 percent more likely to comment on a news story. These metrics should influence your command's content strategies.

Do not feel that you must use multiple platforms. It's far better to have one successful social media site than multiple sites that aren't used effectively.

Official Use of Social Media for Navy Commands

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

! Official use of social media is a public affairs responsibility.

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 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 do not include command or activity websites.

DoDI 8550.01 requires that all official social media presences be registered. Official Navy social media sites need to be registered at *http://www.navy.mil/socialmedia*.

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 Navy presences on social media, to include:

- **Administrators:** Commands and activities shall designate administrators for official use of IbCs in writing. The administrator is responsible for ensuring postings to the IbC 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, which is available at *http://www.navy.mil/socialmedia*.

- **Local Procedures:** Commands and activities must develop written local procedures for the approval and release of all information posted on command and activity official use of IbC.

- **Security:** Commands will actively monitor and evaluate official use of IbC for compliance with security requirements and for fraudulent or unacceptable use.

- **Primary Web Presence:** A command or activity IbC presence, including those on blog platforms, may not serve as the DoN entity's primary web presence and must link to the primary web presence, the command or activity's official website.

- **Prohibited Content:** Commands and activities shall not publish and shall prohibit content such as:

  a. 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.

  b. 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.

Deciding if Social Media is Right for a Command

Social media is not a silver bullet for all of your command's communications needs. Not every command needs a social media presence. It is far better to not start a social media site than to ineffectively use it and abandon the site.

Before launching a social media site, consider what you want to accomplish. What are your communications 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 audiences and use the right social media platform to reach them. Do you want to communicate with your Sailors, Navy civilians, command leadership, family members, the local community, a broader DoD audience, the American public or another group altogether? Do you have the content and personnel – both now and long term – to routinely engage with those audiences?

Additionally, if your command already has a social media presence, you should routinely ask yourself the above questions to ensure it remains an effective communications tool. If it isn't, take the opportunity to address the underlying issues using the best practices in this handbook and at *http://www.navy.mil/socialmedia*. If you are considering no longer using your site, contact CHINFO at *navysocialmedia@navy.mil* before making a decision to discuss the proper way to disestablish the site, or temporarily suspend activity. Your command has developed an online community; you shouldn't suddenly abandon it.

Alternatives

If your command desires 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 that you want to limit to a specific group, consider one of the Navy's 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 command ombudsman, 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 Navy Installations Command, contact the base PAO and/or the Navy region PAO.

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

Do not 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.

If your command is not comfortable sharing its content with the entire world, do not post it on social media. !

Strategy Development

Social media is not a substitute for a public affairs program. As you decide how social media can support it, ask yourself the following questions to begin developing your command's social media strategy.

Audience(s): Who are you trying to reach?

Goal: What will a successful social media site accomplish?

Objectives: What specific steps will you take to reach your goal?

Assessment: How will you decide whether or not your site has reached its goal? How will you know if you are employing effective tactics? How will you know if you are reaching your intended audience(s)?

Content Planning

As public affairs plans are developed, discuss how to gather and produce content that is optimized – both written and visually – for specific platforms based on your command's social media strategy.

A single event such as a change of command ceremony can result in multiple products such as a Navy.mil story, live tweets, a blog from the outgoing and/or incoming commanding officer, and a social media graphic with a quote – all from prepared remarks that can be requested before the ceremony.

Refer to *http://www.navy.mil/socialmedia*
for the latest platform-specific best practices.

Once released, all Navy content is in the public domain and may not include any copyrighted material such as music, photos, videos or graphics.

In addition to deciding what you will create, discuss when and where you will share it. Not all of your content needs to be shared at once and on all of your sites.

For example, content shared on the Navy's Twitter account is frequently not shared on Facebook and vice versa. The Twitter account is a blend of news about the Navy and relevant trending content related to the Navy that attracts new followers. Additionally, the posting frequency is different. Since Twitter is about what's happening in the moment, content is tweeted more often than posted on Facebook. When content about a single topic is shared on Facebook and Twitter, it is optimized for that platform. The tweet is much more concise and shorter (due to Twitter's 280-character limit) and includes relevant hashtags and mentions of other Twitter users. Visually, the supporting imagery is edited by size and duration for each platform.

Social media sites display images in different sizes.
Recommended dimensions are available at
***http://www.navy.mil/socialmedia*.**

Once you've developed your content plan, update your content calendar.

It can be tempting to connect, for example, a Facebook account to a Twitter account so they automatically post to each other. However, while it will save you time, it is not an effective approach. Instead, it is an indicator that you likely do not have the personnel and content to sustain more than one site.

Commands are responsible for official content posted on their social media. Like a press release or content posted to a Navy website, information posted to an official social media presence must be approved by a release authority. Contractors may help manage a social media presence, but they cannot serve as a spokesperson for the Navy. Therefore, a Navy release authority must review and approve all content prior to a contractor posting it.

This is an example of CHINFO's content calendar:

Friday, Dec. 15, 2017

Facebook

Time	Type	Post	Content Theme	Author	Status
945	Facebook Live	Some families are getting an early Christmas present today... a Sailor who will be forged by the sea. Watch our newest Sailors graduate boot camp live!	People	JK	Posted (Approved by CM)
1715	Facebook video	Before you watch the commissioning of the Freedom-variant littoral combat ship USS Little Rock (LCS 9) this Saturday at 11A ET on our Facebook page, here's a video to help you get to know her, now.	Platforms	JK	Scheduled (Approved by CM)

Twitter

Time	Type	Tweet	Content Theme	Author	Status
0725	Link with photo	LIVE 9:45AM ET: Watch #USNavy's newest Sailors graduate boot camp – http://navylive.dodlive.mil/2017/12/15/navy-recruit-graduation-december-15-2017	People	JK	Posted (Approved by CM)
0945	Link with photo	LIVE NOW: Watch #USNavy's newest Sailors graduate boot camp – http://navylive.dodlive.mil/2017/12/15/navy-recruit-graduation-december-15-2017	People	JK	Posted (Approved by CM)
1350	Twitter video	That #FridayFeeling when our newest Freedom-variant littoral combat ship, future #USSLittleRock #LCS9, is just a day away from joining our #USNavy fleet	Platforms	JK	Scheduled (Approved by CM)

Navy Live blog

Time	Type	Tweet	Content Theme	Author	Status
0001	Webcast via DVIDS	Navy Recruit Graduation: December 15, 2017 http://navylive.dodlive.mil/2017/12/15/navy-recruit-graduation-december-15-2017	People	JK	Posted (Approved by CM)

Crisis Communication: Casualties and Adverse Incidents

Social media is a major part of most people's lives during the good times and the bad times. Using social media to communicate with stakeholders during a crisis has proven to be effective due to its speed, reach and direct access. Social media distributes official information and also facilitates dialogue among the affected and interested parties.

If you can release information to the media, you can release the same information via your social media channels. As you develop the crisis communication portion of your public affairs guidance and plans, include possible social media posts and tweets with your traditional holding statements.

Once you become aware of a potential or confirmed adverse incident, casualty or crisis, immediately cancel all scheduled content so you do not appear disconnected from or insensitive to the situation.

Casualties

When personnel are killed, wounded or missing in action, it is hard to control the flow of information distributed through social media platforms. While it is difficult to prepare for these situations, it is important to know that social media can play a role (good or bad).

The media may look at command, Sailor, DoN civilian and family member social media to get more information. It is important that privacy settings are regularly reviewed to be as restricted as practical. It's too late during a crisis.

It is vitally important that all Sailors, DoN civilians, family members and friends know that the identity of a casualty should not be discussed on social media until it has been released. In accordance with DoDI 1300.18, Department of Defense (DoD) Personnel Casualty Matters, Policies and Procedures, 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 next of kin regarding the casualty status of the member. 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.

Adverse incidents

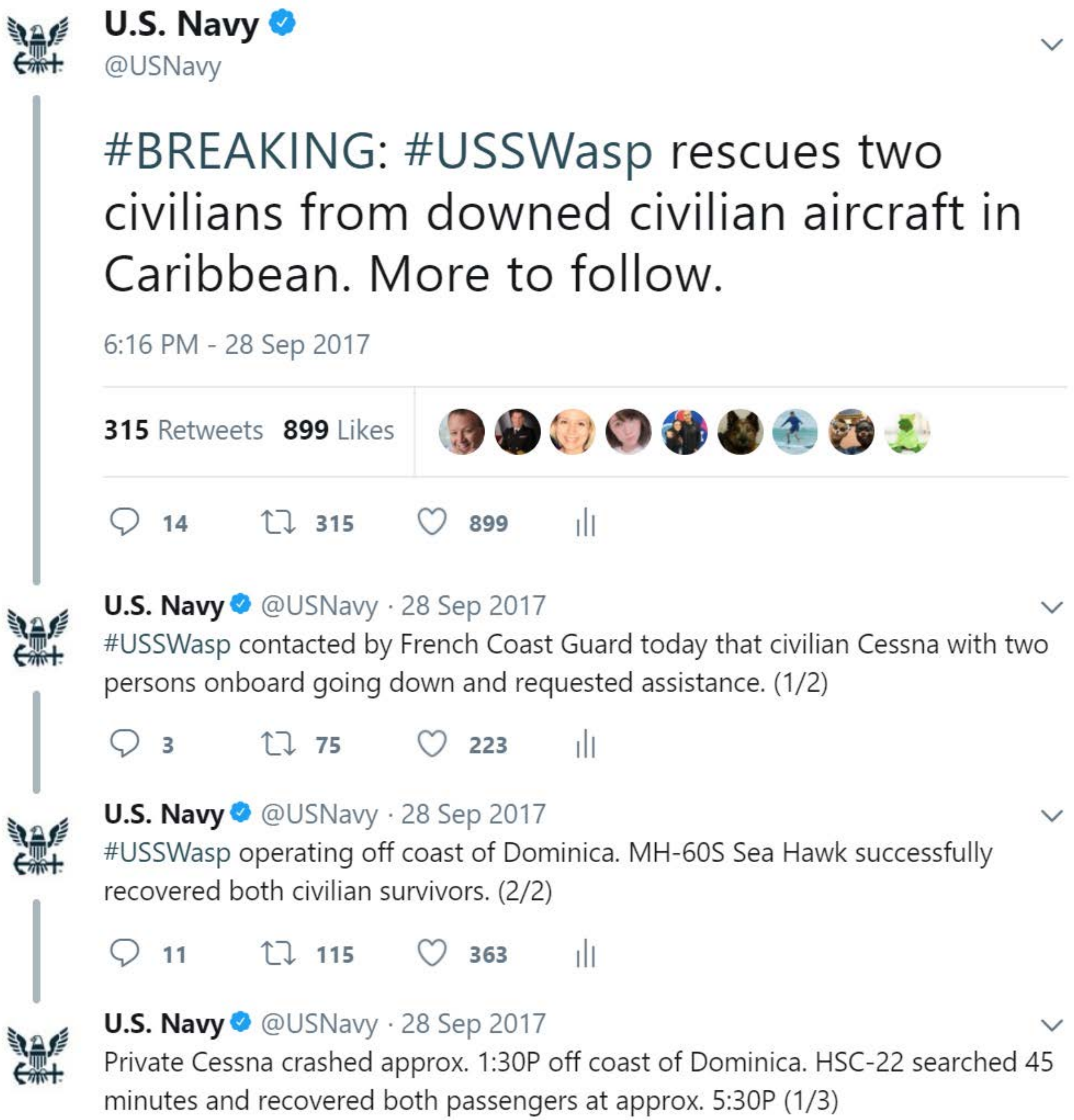
The time to start using social media isn't during a crisis. In order to build credibility, you need to establish a social media presence before a crisis. A large social media following doesn't happen overnight, so relax and execute your social media strategy. The better you are at providing good information 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 such as a hurricane, tell your audience where they should go for the latest information.

Post information as it is released

Social media moves information quicker than ever, so when a crisis hits, don't wait for a complete formal press release. When you have released information, post it. You can always post additional information as it is released. If you expect that you will provide updates, say so. Not posting timely updates during a crisis may damage the command's credibility.

While the below examples are from Twitter, the same principles apply for other social media platforms.



U.S. Navy
@USNavy

#BREAKING: #USSWasp rescues two civilians from downed civilian aircraft in Caribbean. More to follow.

6:16 PM - 28 Sep 2017

315 Retweets 899 Likes

14 315 899

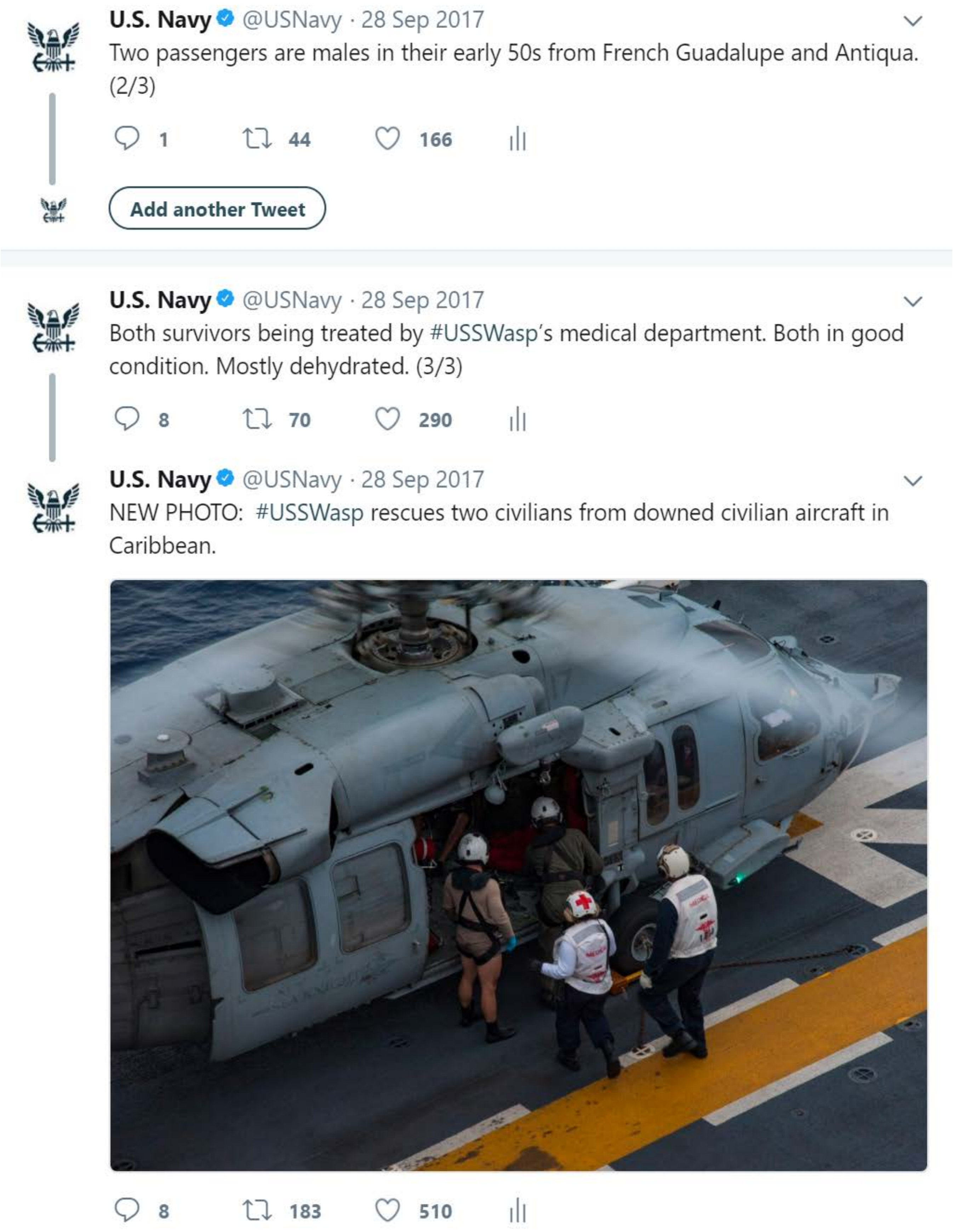
U.S. Navy @USNavy · 28 Sep 2017
#USSWasp contacted by French Coast Guard today that civilian Cessna with two persons onboard going down and requested assistance. (1/2)

3 75 223

U.S. Navy @USNavy · 28 Sep 2017
#USSWasp operating off coast of Dominica. MH-60S Sea Hawk successfully recovered both civilian survivors. (2/2)

11 115 363

U.S. Navy @USNavy · 28 Sep 2017
Private Cessna crashed approx. 1:30P off coast of Dominica. HSC-22 searched 45 minutes and recovered both passengers at approx. 5:30P (1/3)



U.S. Navy @USNavy · 28 Sep 2017

Two passengers are males in their early 50s from French Guadalupe and Antiqua. (2/3)

1 44 166

U.S. Navy @USNavy · 28 Sep 2017

Both survivors being treated by #USSWasp's medical department. Both in good condition. Mostly dehydrated. (3/3)

8 70 290

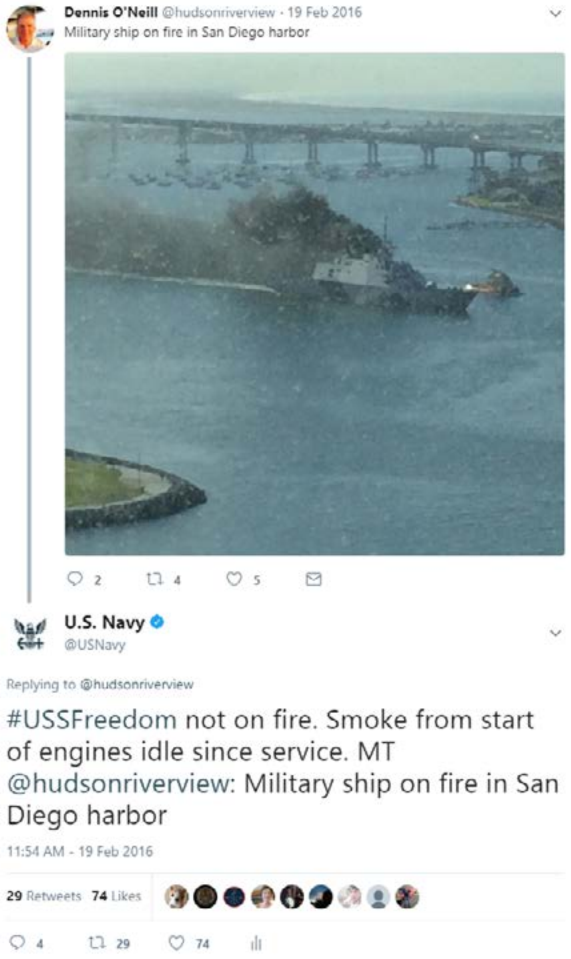
U.S. Navy @USNavy · 28 Sep 2017

NEW PHOTO: #USSWasp rescues two civilians from downed civilian aircraft in Caribbean.

8 183 510

Correct the record

This next example is a reminder to be prepared to respond to misinformation and rumors before they become a widespread conservation.



Dennis O'Neill @hudsonriverview · 19 Feb 2016

Military ship on fire in San Diego harbor

2 4 5

U.S. Navy @USNavy

Replying to @hudsonriverview

#USSFreedom not on fire. Smoke from start of engines idle since service. MT @hudsonriverview: Military ship on fire in San Diego harbor

11:54 AM - 19 Feb 2016

29 Retweets 74 Likes

4 29 74

If the Navy had not replied with a coordinated response, this single tweet may have gained traction. It would've been much more difficult to correct multiple tweets and any possible media reports.

It's also important to note that this information was limited to Twitter. So, there was no need to address it on any other platform.

Analyze results

Once the crisis is over, analyze what happened. Evaluate metrics and track user feedback. It is important to evaluate how a social media presence performs during a crisis so adjustments can be made for the future.

Case study: Washington Navy Yard shooting

The public and private sector – including Twitter – cited the Navy's use of Twitter during and after the Washington Navy Yard shooting as a best practice to keep the public up-to-date during a fast-moving news situation.

In its analysis, Twitter found @USNavy became the "official source of information for followers and the media," and guided the online conversation by creating the hashtag #NavyYardShooting, which resulted in 1,900 related tweets per minute at the peak of the story.

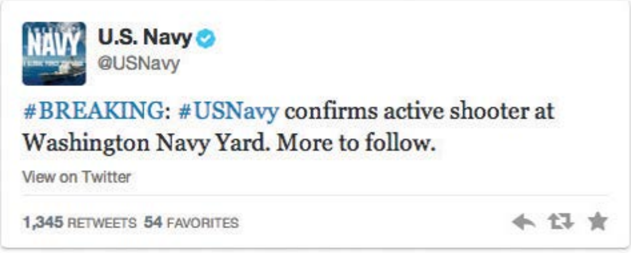
Build relationships. Don't wait for something big to happen to get familiar with the public affairs officer in charge of media queries, build relationships on Twitter with your local media, know who your social media influencers are and communicate with them often. If you wait until you need someone to get to know them, you've waited too long.

Have a well-trained team. Be comfortable using Twitter before a crisis. Even if you're the Twitter guru on your team, make sure the rest of your colleagues understand how to use the platform. For the Navy Yard incident, CHINFO had four people dedicated to various Twitter related tasks. So, set up a training session, have your colleague sit beside you when you draft tweets and recommend some reading. Make sure you have people in your office, other than yourself, that you trust to tweet on behalf of your command. You never know when you will need the help.

Be able to react quickly. The first step in a crisis situation is confirmation. You may not know all the details, and that's okay, but the people involved and the media want information. The days of waiting for that perfectly polished press release are over. News is happening and it's happening now.

Instead of waiting to release a statement until you have the full story, ask yourself, "What do you know now?" This is where being a trusted advisor is critical. Talk to leadership and emphasize the need to get out ahead of the press release with confirmed and releasable facts, but remember speed does not replace the need for accuracy.

For the Washington Navy Yard shooting, we knew there was an active shooter, we knew the location and we knew about our people. The ability to tweet that information once released – even before the full press release was complete – helped to frame the story and controlled misinformation. Additionally, since we knew there would be frequent updates, we told the media to monitor the Navy's Twitter account for the latest information.


U.S. Navy
@USNavy

#BREAKING: #USNavy confirms active shooter at Washington Navy Yard. More to follow.

View on Twitter

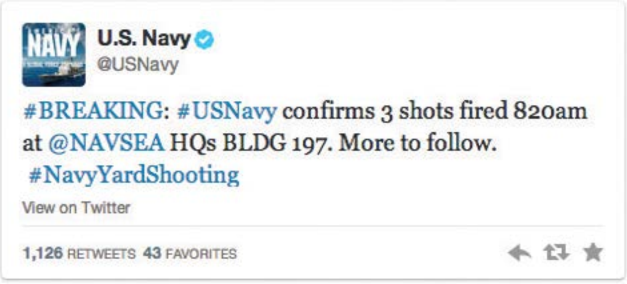
1,345 RETWEETS 54 FAVORITES

Sending tweets is only half of your job. Twitter is complex. A lot is happening all the time and it's hard to keep up without diligently monitoring. CHINFO has several established monitoring streams that we check multiple times throughout the day, but in an instance like the Washington Navy Yard shooting, they weren't enough. Set up the following streams that you and your team should monitor daily:

- Mentions of your account's handle (e.g., @USNavy)
- Your retweets
- Keywords associated with your command. We know not everyone uses our handle (@USNavy) so we also search for mentions of Navy, USNavy, #USNavy and U.S. Navy
- Campaign or incident specific keyword searches (e.g., "Navy + aircraft")

In a crisis situation, we adapt and add streams based on how people are talking about the incident. During the shooting, we started the hashtag #NavyYardShooting to make it easier to group and track conversations about the incident, but we also monitored mentions of "Navy + shooting."

One voice. When something of this scale happens, it's best to present one, united and informed Navy voice to the public. There will be a lot of questions. People will dig for information. It's your job to identify the right voice. Identifying and directing people to the appropriate spokesperson and online source of information will go a long way to help minimize misinformation.


U.S. Navy
@USNavy

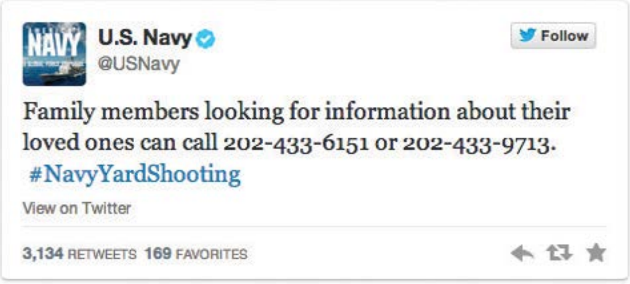
#BREAKING: #USNavy confirms 3 shots fired 820am at @NAVSEA HQs BLDG 197. More to follow. #NavyYardShooting

View on Twitter

1,126 RETWEETS 43 FAVORITES

During the shooting, @USNavy was the "digital spokesperson" for the most part, but conflicting reports occurred from on-scene accounts. Some of these reports were untrue or unconfirmed at the time. Multiple Navy spokespersons were then quoted, which caused confusion and made @USNavy tweets appear uncoordinated.

Have a plan. Crisis situations often follow a bell curve. There was a point where conversations decreased and stabilized. Once that occurs, there isn't a need to post minute-by-minute updates, but you should still be an active participant in the conversations.


U.S. Navy
@USNavy

Follow

Family members looking for information about their loved ones can call 202-433-6151 or 202-433-9713. #NavyYardShooting

View on Twitter

3,134 RETWEETS 169 FAVORITES

For days following the shooting, there were spikes in conversations when new information was released. Additionally, there will still be people wanting more information. Continue to monitor and be ready to direct people to the correct point of contact for more information on your topic.

Account Security

Official Navy Facebook pages must be attached to individuals' Facebook profiles. Do not share 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 granted access, updates to the command's Facebook page will be posted as the page and not the individuals.

For other social media sites, use your command PAO's general Navy.mil email address to create an official account. Generate a secure password and share it only with account administrators.

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

Passwords should be unique for each platform, and difficult to guess and ideally created through a random password generator. Only share the password with people who are authorized to manage the account, and change the passwords regularly.

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:

1. Timing is critical in these initial minutes. First, complete a support request through the social media site. Simultaneously, notify your higher command's PAO and your command's security officer. Then, immediately contact CHINFO. During regular working hours, call Navy Media Content Operations at 703-614-9154. Outside of regular working hours, contact the CHINFO duty officer at 703-850-1047 and request assistance from the digital media team.
2. Change all other social media passwords. Even if you think the security breach is limited to the one account, it is prudent to change the passwords of all other social media accounts. If you've lost control of other accounts, contact those platforms immediately also and CHINFO. You should also change the passwords on your personal accounts.
3. If you don't have access to your account yet, use other accounts to alert your online community that a breach occurred. The right words and speed matter. Regardless of whether you have access, carefully decide what you will say. The same rules for crisis communication offline apply online. Remember a traditional 24-hour news cycle offline can occur in just a few minutes online.
4. Once you've regained control of your account, change your password and screen shot the unauthorized content before deleting it.

Operations Security (OPSEC)

We all know that "Loose Lips Sink Ships" and social media amplifies OPSEC risks because it enables greater volume and increased speed of information shared publicly. Navy communicators should carefully consider the level of detail used when posting information anywhere on the internet, and should err on the side of taking a cautious and conservative approach. Local procedures should be established to ensure that all information posted on social media is releasable and in accordance with local public affairs guidance and Navy Public Affairs Regulations. It is then the responsibility of the social media managers to identify information that may compromise OPSEC and remove it.

Navy communicators must also inform Sailors and DoN civilians as well as their families, and their command's online community of OPSEC best practices:

1. **Deployment:** You should minimize the risk of sharing information related to a current deployment. Instead of saying, "My Sailor is in ABC unit at DEF camp in GHI city in Afghanistan" loved ones should rephrase it to: "My Sailor is in Afghanistan." Close family and friends should already know this information if they're allowed, so there is no need to post it online.
2. **Schedules:** Posts about scheduled movements and current or future locations should be avoided. "She is coming home," should be used instead of saying, "She will be back on X date from ABC city." Generally, it is safer to talk about events that have happened – not that will happen unless that information has been released to the media.
3. **Personal Information:** Limit personal information such as deployment status, addresses, telephone number, location information, schedules, family members (e.g., names, addresses, birth dates, birthplace, local towns, schools, etc.), etc.
4. **Friends:** Everyone should be careful who they friend on social media and who follows them. Not everyone who wants to be a friend or follower is necessarily who they claim to be. Be mindful of others attempting to use social presences as a means of targeting individuals. Only allow people who are known in real life into social circles.

Other information that should not be shared by anyone includes descriptions of military facilities, unit morale, future operations or plans, results of operations, technical information, details of weapons systems, equipment status, and well as the discussion of daily routines and frequently visited locations.
Everyone should be encouraged to post about the following: pride and support for service members, units and specialties; generalizations about service or duty; port call information after it has been released to the media; general status of the location of a ship at sea (e.g., operating off the coast of San Diego, as opposed to 45 nm north of San Diego); and content from official Navy social media sites.

Navy social media managers should do the following if they identify OPSEC violations:

1. Record and archive the information, and remove it if possible.
2. Notify the command's PAO and security officer of any potential OPSEC violation.
3. Inform the user of the OPSEC violation. Use it as a teachable moment and provide them with OPSEC best practices and resources so they don't repeat the mistake.
4. Educate the online community about OPSEC, why it is important and what they can do if they think they know of a violation.

Politics and Endorsements

Navy accounts should only like official government social media accounts.

Navy accounts are forbidden from expressing opinions about public issues, including, but not limited to, politics, political candidates, elected officials and political parties. Similarly, official Navy accounts should not like or follow partisan accounts, including, but not limited to, accounts belonging to a specific political party or political candidate.

The government does not allow solicitations or advertisements of any kind. This includes promotion or endorsement of any financial, commercial or non-governmental agency. Similarly, attempts to defame or defraud any financial, commercial, or non-governmental agency are prohibited.

Online Advertising

With very few exceptions, Navy accounts may not pay to boost Facebook posts, promote tweets or take similar action on content.

Navy communicators may not engage in advertisement 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 JAG or contracting officer for exceptions and additional information.

Online Conduct

Any member of the Navy community who experiences or witnesses incidents of improper online behavior should promptly report it to their chain of command via the Command Managed Equal Opportunity manager or Fleet and Family Support office. Additional avenues for reporting include Equal Employment Opportunity offices, the Inspector General, Sexual Assault Prevention and Response offices and 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.

Specific instructions are available at *http://www.ncis.navy.mil/pages/NCISTips.aspx*.

Refer to the handbook's *appendix* for additional information.

Impersonators

Regularly search for impostors and report them to the social media site.

The impersonation of a senior Navy official, such as a flag officer or a commanding officer, should also be reported to CHINFO at 703-614-9154 and *navysocialmedia@navy.mil*.

Ensure your official Navy social media site has been registered as required at *http://www.navy.mil/socialmedia*. If you discover a social media site that portrays itself as an official Navy site, contact CHINFO.

SAILORS

Sailors have always been ambassadors of the Navy in their actions and words, both at home and overseas. With that role in mind, it is important for you to understand what it means to communicate online to ensure you are responsibly representing the Navy.

It has never been simpler for a Sailor to reach a large, public audience intentionally or unintentionally through email, social media, blogs and other platforms. While most Sailors do not work in public affairs and do not officially speak on behalf of the Navy, all Sailors must recognize that they still may be perceived as a spokesperson for the Navy simply because they wear a Navy uniform.

As a Sailor, you are often the best spokesperson the Navy has; you can share a direct, unfiltered perception of what it means to serve your country and can provide personal insights into life in the Navy. However, you do not always have complete control to decide when you are and are not speaking for the Navy, so you must understand how to communicate responsibly as an individual, taking care not to do or say anything to cast yourself or the Navy in a negative or unintended light.

This handbook will teach you some of the best practices that you should follow while using social media.

Online Conduct

No Sailor should communicate on social media or elsewhere in a way that may negatively impact herself or himself or the Navy. It is often hard to distinguish between the personal and the professional on the internet, so Sailors should assume that any content they post may impact their personal careers and the reputation of the Navy more broadly. Sailors should not engage in any conversations or activities that may threaten the Navy's core values or operational readiness.

Content that is defamatory, threatening, harassing, or discriminating on the basis of race, color, sex, gender, age, religion, national origin, sexual orientation or any other protected criteria is punishable and should be avoided. The internet doesn't forget; online habits leave digital footprints. Take caution when posting content, even if you think you are doing so in a private and closed community.

Follow the UCMJ

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

Punitive action may include Articles 88, 89, 91, 92, 120b, 120c, 133 or 134 (General Article provisions, Contempt, Disrespect, Insubordination, Indecent Language, Communicating a threat, Solicitation to commit another Offense, and Child Pornography offenses), as well as other articles, including Navy Regulations Article 1168, nonconsensual distribution or broadcast of an intimate image.

Behaviors with legal consequences include:

- Child exploitation/Child sexual exploitation
- Computer misuse (hacking)
- Cyber stalking
- Electronic harassment
- Electronic threats
- Obscenity

Reporting Incidents

Any member of the Navy community who experiences or witnesses incidents of improper online behavior should promptly report it to their chain of command via the Command Managed Equal Opportunity manager or Fleet and Family Support office. Additional avenues for reporting include Equal Employment Opportunity offices, the Inspector General, Sexual Assault Prevention and Response offices and 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.

Specific instructions are available at *http://www.ncis.navy.mil/pages/NCISTips.aspx*.

Refer to the handbook's *appendix* for additional information.

Politics

Active-duty Sailors may generally express their personal views about public issues or political candidates using social media — just like they can write a letter to a newspaper's editor. If the social media site or content identifies the Sailor as on active duty (or if they're reasonably identifiable as an active-duty Sailor), then the content needs to clearly and prominently state that the views expressed are those of the individual only and not those of the Department of Defense. However, active-duty service members may not engage in any partisan political activity such as posting or making direct links to a political party, partisan political candidate, campaign, group or cause. That's the equivalent of distributing literature on behalf of those entities or individuals, which is prohibited.

Active-duty Sailors can like or follow accounts of a political party or partisan candidate, campaign, group or cause. However, they cannot suggest that others like, friend or follow them or forward an invitation or solicitation.

Remember, active-duty service members are subject to additional restrictions based on the Joint Ethics Regulation, the Uniform Code of Military Justice and rules about the use of government resources and government communications systems, including email and internet.

What about Sailors who aren't on active duty? They're not subject to the above social media restrictions so long as they don't reasonably create the perception or appearance of official sponsorship, approval or endorsement by the DoD.

The information above doesn't cover everything. If in doubt, consult your command's ethics counselor.

!

Cybersecurity

One of the best features of social media sites is the ability to connect people from across the world in spontaneous and interactive ways. However, this also opens its users and their systems to security weaknesses. Information shared on the internet can provide adversaries such as terrorists, spies and criminals with information that may be used to harm you or disrupt your command's mission. Remember, hacking, configuration errors, social engineering and the sale/sharing of user data mean your information could become public at any time.

You should choose passwords that are unique and difficult to guess for each social media account. You should not share your passwords or security questions. When using computers, you should make sure to regularly update your anti-virus software, and beware of links, downloads and attachments. Look for HTTPS://, the lock icon or a green browser bar that indicate active transmission security before logging in or entering sensitive data (especially when using Wi-Fi hotspots).

Refer to the handbook's *appendix* for additional information.

Operations Security (OPSEC)

We all know that "Loose Lips Sink Ships" and social media amplifies Operations Security risks because it enables greater volume and increased speed of information shared publicly. OPSEC rules are universal and should be maintained online just as they are offline. If you wouldn't say it, write it or type it, don't post it on the internet. OPSEC violations commonly occur when personnel share information with people they do not know well or if their social media accounts have loose privacy settings.

You need to be especially careful when it comes to discussing current deployments, scheduled movements, and current or future locations. Instead of saying, "I'm in Any Unit at Naval Station Anywhere in Any City, Japan," you should rephrase it to say, "I'm deployed in the Pacific." Instead of saying, "I will be back in 53 days" you should say "I am coming home." Other information that should not be shared includes: description of bases, unit morale, future operations or plans, results of operations, discussion of areas frequented by service members (even off-duty hangouts), daily military activities and operations, technical information, details of weapons systems and equipment status.

Generally, it is safer to talk about events that have happened – not that will happen – unless that information has been released to the media. Close family and friends should already know details related to your schedule if they're allowed, so there is no need for you to post this online.

As a Sailor, you should also limit the personal information you post about yourself (e.g., deployment status, addresses, telephone number, location information, schedules, etc.) and your family members (e.g., names, addresses, birth dates, birthplace, local towns, schools, etc.).

You should be careful about who you friend on social media and who follows you. Not everyone who wants to be your friend or follower is necessarily who they claim Only allow people who you know in real life into your social circles.

Adverse Incidents

Social media is a major part of most people's lives during the good times and the bad times. When our shipmates are killed, wounded or missing in action, it is hard to control the flow of information distributed through social media platforms. While it is difficult to prepare for these situations, it is important to know that social media can play a role (good or bad) in the handling of a serious illness, injury or death. In accordance with DoDI 1300.18, Department of Defense (DoD) Personnel Casualty Matters, Policies and Procedures, 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 next of kin regarding the casualty status of the member. 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.

Always follow unit protocol when it comes to these situations. It is imperative that you do not add to rumors and speculation. If approached by someone, discuss that you do not know and they should not speculate.

Journalists' jobs are to report the news, which includes adverse incidents. The media may look at command, Sailor, DoN civilian and family member social media to get more information. It is important that privacy settings are regularly reviewed to be as restricted as practical. It's too late when something bad as happened. Should you be contacted by a member of the media, simply refer them to your command's public affairs officer.

Endorsements

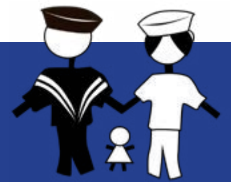
Sailors must not officially endorse or appear to endorse any non-Federal entity, event, product, service or enterprise, including membership drives for organizations and fundraising activities.

You can never solicit gifts or prizes for command events in any capacity – on duty, off duty or in a personal capacity. You may not solicit gifts or prizes for command events.

Bottom line

If you can't say or do it offline, you can't say or do it online.

FAMILIES



If you are reading this, a loved one is affiliated with the U.S. Navy. We are grateful for them and for your dedicated support of their chosen career. One way to support your Sailor is to recognize the importance of sharing the Navy story.

You have likely heard that family readiness equals warfighting readiness, and we hope you believe that as strongly as we do. Without strong, capable families, our Sailors cannot be prepared to do what they must to defend our nation and further our objectives abroad. Because families are such a big part of our Navy, it is crucial that should you choose to share your story, you follow the guidelines to preserve OPSEC and propriety.

This section will teach you some of the best practices that you should follow on social media.

Cybersecurity

One of the best features of social media sites is the ability to connect people from across the world in spontaneous and interactive ways. However, this also opens its users and their systems to security weaknesses. Information shared on the internet can provide adversaries such as terrorists, spies and criminals with information that may be used to harm you or disrupt your command's mission. Remember, hacking, configuration errors, social engineering and the sale/sharing of user data means your information could become public at any time.

Anyone using social media should choose passwords that are unique and difficult to guess for each account. You should not share passwords or security questions. Regularly update your anti-virus software and operating system to install the latest security patches, and beware of links, downloads and attachments. Look for HTTPS://, the lock icon or a green browser bar that indicate active transmission security before logging in or entering sensitive data (especially when using Wi-Fi hotspots).

Operations Security (OPSEC)

You might have heard the saying that "Loose Lips Sink Ships" and social media amplifies Operations Security risks because it enables greater volume and increased speed of information shared publicly. OPSEC violations commonly occur when someone shares information with people they do not know well (like their Twitter followers), or if their social media accounts have loose privacy settings.

Families of Sailors need to be especially careful when it comes to discussing current deployments, scheduled movements, and current or future locations. Instead of saying, "My son, IT2 Any Sailor, is in Any Unit at Naval Station Anywhere in Any City, Japan," you should rephrase it to say, "My Sailor is deployed in the Pacific." Instead of saying, "My Sailor will be back in 53 days" you should say "My Sailor is coming home."

You should also limit the personal information you post about yourself (e.g., names, addresses, birth dates, birthplace, local towns, schools, etc.) or your Sailor (e.g., deployment status, addresses, telephone number, location information, schedules, etc.).

! **To be safer, talk about events that have happened – not that will happen unless that information has been released to the media.**

Dangerous	Safer
My son, IT2 Any Sailor, is in Any Unit at Naval Station Anywhere in Any City, Japan.	My Sailor is deployed in the Pacific.
My daughter, Ens. Any Sailor, is aboard USS John C. Stennis. She's coming home in 53 days.	My daughter's ship is coming home in a couple of months.
My family is in Houston, Texas	I'm from Texas.

Family members should be careful who they friend on social media and who follows them. Not everyone who wants to be your friend or follower is necessarily who they claim. Only allow people that you actually know in real life into your social circles.

As a family member of a Sailor, you should feel free to post about pride and support for service members, port call information after it has been released to the media, general status of the location of a ship at sea (e.g., operating off the coast of San Diego, as opposed to 45 nm north of San Diego), and posts from official Navy social media presences.

Adverse Incidents

Social media is a major part of most people's lives during the good times and the bad times. When Sailors are killed, wounded or missing in action, it is hard to control the flow of information distributed through social media platforms. While it is difficult to prepare for these situations, it is important to know that social media can play a role (good or bad) in the handling of a serious illness, injury or death.

In accordance with DoDI 1300.18, Department of Defense (DoD) Personnel Casualty Matters, Policies and Procedures, 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 next of kin regarding the casualty status of the member. 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.

It is imperative that you do not add to rumors and speculation when there is a report of an injury or death. If approached by someone, explain that you do not know and they should not speculate.

Journalists' jobs are to report the news, which includes adverse incidents. The media may look at command, Sailor, DoN civilian and family member social media to get more information. It is important that privacy settings are regularly reviewed to be as restrictive as practical. It's too late when something bad has happened. Should you be contacted by a member of the media, simply refer them to your command's public affairs officer.

OMBUDSMEN

Thank you for taking on the vital role as an command ombudsman. You are a vital link between the command's leadership and families.

You have likely heard that family readiness equals warfighting readiness, and we hope you believe that as strongly as we do. Without strong, capable families, our Sailors cannot be prepared to do what they must to defend our nation and further our objectives abroad. Because families are such a big part of the Navy's story, it is crucial that you – as an ombudsman – share your Navy story and encourage Navy families to do the same.

Be sure to follow the Navy Ombudsman At Large Facebook page at https://www.facebook.com/USNavyOmbudsmanAtLarge.

This section will teach you some of the best practices that you should follow while supporting your command and encouraging others to do the same.

Overview of Today's Landscape

Social media usage is nearly universal among younger adults and is quickly growing among people over age 50. People use it to consume news, make or strengthen connections and engage in discussions and activism related to personal interests. There are many different social media platforms, each with distinct use cases that are preferred by different types of people.

Best Practices to Support Command's Official Social Media Presence(s)

When ships or units are deployed, they have less bandwidth or no connection at all, which makes it difficult or impossible to update social media sites. Having someone shore side to help post released updates, photos and videos can be extremely helpful. We recommend that you talk to the public affairs officer or senior enlisted advisor before the command deploys and discuss this possibility. Ask the public affairs officer for training before he or she departs in case they need your support.

Social media is most valuable when community members engage in discussions, share resources and network. As the ombudsman, you are in an excellent position to encourage discussion. People will be honest, ask questions – and at times – may express frustration. This feedback enables the command leadership and you to effectively address family concerns. More often than not, we have seen overwhelmingly supportive Navy families on social media – especially when there is an active and responsive account administrator.

You and the command can consider a number of options to support family readiness through social media. We recommend that commands have a single presence on any given social media platform, with the ombudsman actively participating. Go to your audience – your families. It is up to you and your command to determine what social media platform is the best fit for how you need to communicate with your families.

Social media can be viral. So, it is easy to post information in one place and for it to quickly spread to your command's extended family. A well-coordinated command social media presence with active participation from you alongside command leadership, presents a cohesive and supportive environment that leads to stronger family readiness.

If the command is unable to support a social media presence on a long-term basis, we recommend it doesn't create one. It is far better to not start a social media site than to ineffectively use it and abandon the site. However, remember that people want to communicate with one another. Your families can and will create their own social media presences if the command does not have one. It is in your best interest and the command's to lead the way by providing an online presence for your families.

Many commands have unofficial social media presences established by former crew members, veterans or fans excited about the command. Work with the command leadership to determine if you want to approach the presence and/or simply monitor it and chime in when you have information to add. You may want to contact the administrator to see how you can work together. Regardless, this should not stop you or the command from creating an official presence for the command and its families. These official presences are listed in the Navy Social Media Directory (lists only command presences, not family readiness groups) which can be found at *http://www.navy.mil/socialmedia*. If you find an online presence portraying itself as an official presence and the command is not sponsoring it, your command's public affairs officer should contact the Navy Office of Information at *navysocialmedia@navy.mil*.

If you are turning over your ombudsman duties, teach the incoming ombudsman how the social media account works and explain how you've been using it. Then, introduce the new ombudsman on the platform and send a sign-off message. You may also recommend the new ombudsman post a photo and/or note introducing himself or herself. Finally, ensure you have made them an account administrator (Facebook) and/or given them the account's username and password (other platforms).

Cybersecurity

One of the best features of social media sites is the ability to connect people from across the world in spontaneous and interactive ways. However, this also opens its users and their systems to security weaknesses. Information shared on the internet can provide adversaries such as terrorists, spies and criminals with information that may be used to harm you or disrupt your command's mission. Remember, hacking, configuration errors, social engineering and the sale/sharing of user data means your information could become public at any time.

Anyone using social media should choose passwords that are unique and difficult to guess for each account. You should not share passwords or security questions. Regularly update your anti-virus software and operating system to install the latest security patches, and beware of links, downloads and attachments. Look for HTTPS://, the lock icon or a green browser bar that indicate active transmission security before logging in or entering sensitive data (especially when using Wi-Fi hotspots).

Refer to the handbook's *appendix* for additional information.

Operations Security (OPSEC)

You've likely heard the saying that "Loose Lips Sink Ships" and social media amplifies Operations Security risks because it enables greater volume and increased speed of information shared publicly. OPSEC violations commonly occur when someone shares information with people they do not know well (like their Twitter followers), or if their social media accounts have loose privacy settings.

Families of Sailors need to be especially careful when it comes to discussing current deployments, scheduled movements, and current or future locations. Instead of saying, "My son, IT2 Any Sailor, is in Any Unit at Naval Station Anywhere in Any City, Japan," you should rephrase it to say, "My Sailor is deployed in the Pacific." Instead of saying, "My Sailor will be back in 53 days" you should say "My Sailor is coming home."

You should also limit the information you post about yourself (e.g., names, addresses, birth dates, birthplace, local towns, schools, etc.). Carefully consider who you friend on social media and who follows them. Not everyone who wants to be your friend or follower is necessarily who they claim. Only allow people that you actually know in real life into your social circles.

If you have any questions about what may violate Operations Security, contact your command's public affairs officer before posting or sharing. !

Ombudsmen should feel free to post about pride and support for service members, port call information after it has been released to the media, general status of the location of a ship at sea (e.g., operating off the coast of San Diego, as opposed to 45 nm north of San Diego), and posts from official Navy social media presences.

You may find yourself educating families about OPSEC and reminding them to be aware of what they post online. Some techniques that might help include:

- Including notes and OPSEC reminders, as well as real-world examples, in monthly newsletters
- Proactively providing information about family readiness group meetings and other appropriate venues to discuss homecoming and port information, so family members do not feel like they have to violate OPSEC; they know where to get information
- Creating a teachable moment when someone violates OPSEC by discussing it with them and others so the mistake is not repeated.

Adverse Incidents

Social media is a major part of most people's lives during the good times and the bad times. When Sailors are killed, wounded or missing in action, it is hard to control the flow of information distributed through social media platforms. While it is difficult to prepare for these situations, it is important to know that social media can play a role (good or bad) in the handling of a serious illness, injury or death.

In accordance with DoDI 1300.18, Department of Defense (DoD) Personnel Casualty Matters, Policies and Procedures, 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 next of kin regarding the casualty status of the member. 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. It is important that all friends, family and fellow Sailors know that information must not be released anywhere, including on private social media accounts, before the next of kin is notified. Always follow unit protocol when it comes to these situations.

Journalists' jobs are to report the news, which includes adverse incidents. The media may look at command, Sailor, DoN civilian and family member social media to get more information. It is important that privacy settings are regularly reviewed to be as restrictive as practical. It's too late when something bad has happened. Should you be contacted by a member of the media, simply refer them to your command's public affairs officer.

Private Groups

Closed, private and unlisted social media groups may sound appealing since they appear to offer a sense of privacy. However, never assume that anything on the internet is truly private. The internet doesn't forget. Content is archived and traceable forever. Take caution when posting content, even if you think you are doing so in a private and closed community.

DEPARTMENT OF THE NAVY CIVILIANS

Cybersecurity

One of the best features of social media sites is the ability to connect people from across the world in spontaneous and interactive ways. However, this also opens its users and their systems to security weaknesses. Information shared on the internet can provide adversaries such as terrorists, spies and criminals with information that may be used to harm you or disrupt your command's mission. Remember, hacking, configuration errors, social engineering and the sale/sharing of user data mean your information could become public at any time.

Anyone using social media should choose passwords that are unique and difficult to guess for each account. You should not share passwords or security questions. Regularly update your anti-virus software and operating system to install the latest security patches, and beware of links, downloads and attachments. Look for HTTPS://, the lock icon or a green browser bar that indicate active transmission security before logging in or entering sensitive data (especially when using Wi-Fi hotspots).

Refer to the handbook's *appendix* for additional information.

Operations Security (OPSEC)

You've likely heard the saying that "Loose Lips Sink Ships" and social media amplifies Operations Security risks because it enables greater volume and increased speed of information shared publicly. OPSEC violations commonly occur when someone shares information with people they do not know well (like their Twitter followers), or if their social media accounts have loose privacy settings.

Be careful when discussing current deployments, scheduled movements, and current or future locations. Other information that should not be shared by anyone includes descriptions of military facilities, unit morale, future operations or plans, results of operations, technical information, details of weapons systems, equipment status, and well as the discussion of daily routines and frequently visited locations. Generally, it is safer to talk about events that have happened – not that will happen – unless that information has been released to the media. Close family and friends should already know details related to your schedule if they're allowed, so there is no need for you to post this online.

Limit the personal information you post about yourself (e.g., addresses, telephone number, schedules, etc.) and your family members (e.g., names, addresses, birth dates, birthplace, local towns, schools, etc.).

You should be careful about who you friend on social media and who follows you. Not everyone who wants to be your friend or follower is necessarily who they claim. Only allow people who you know in real life into your social circles.

Feel free to post about pride and support for service members, port call information after it has been released to the media, general status of the location of a ship at sea (e.g., operating off the coast of San Diego, as opposed to 45 nm north of San Diego), and posts from official Navy social media presences.

Online Conduct

As a Navy civilian, it is important to know that when you're online you still represent the Navy. Online bullying, hazing, harassment, stalking, discrimination, retaliation and any other type of behavior that undermines dignity and respect are not consistent with Navy core values and negatively impact the force.

! Navy civilians can be subject to appropriate disciplinary actions.

Politics

Before posting about politics on social media, Department of the Navy civilians need to consider the Hatch Act and DoD policy. In general, as a federal employee, you may use social media and comply with the Hatch Act if you:

- Don't engage in political activity while on duty or in the workplace, even if you are using your personal smartphone, tablet, or laptop to do so. Federal employees are "on duty" when they're in a pay status (including during telework hours, but not including paid leave) or are representing the government in an official capacity.
- Don't engage in political activity in an official capacity at any time. Political activity refers to any activity directed at the success or failure of a political party or partisan political group or candidate in a partisan race.
- Don't solicit or receive political contributions at any time.

As a civilian, you may express your opinions about a partisan group or candidate in a partisan race by posting, liking, sharing, tweeting or retweeting, but there are a few limitations. The Hatch Act prohibits federal employees from:

- Referring to your official titles or positions while engaged in political activity at any time; it is important to note that including your official title or position in your social media profile is not an improper use of official authority.
- Suggesting or asking anyone to make political contributions at any time, including providing links to the political contribution page of any partisan group or candidate in a partisan race or liking, sharing, or retweeting a solicitation from one of those entities.
- Liking, sharing, or retweeting an invitation to a political fundraising event; however, you may accept an invitation to a political fundraising event from such entities via social media.

Civilians that fall in the "further restricted employees" category may express their opinions about a partisan group or candidate in a partisan race by posting or sharing content, but there are a few limitations.

In addition to the limitations above, the Hatch Act prohibits further restricted employees from:

- Posting or linking to campaign or other partisan material of a partisan group or candidate in a partisan race
- Sharing those entities' social media sites or their content, including retweeting

Civilians are allowed to identify their political party affiliation in their social media profiles, even if it also contains their official title or position, without more. As a civilian, you may display a political party or campaign logo or a candidate photograph in your profile picture, but it is subject to the following limitations. Because a profile picture accompanies most actions on social media, while in the workplace you would not be permitted to post, share, tweet, or retweet any social media content because each such action would show your support for a partisan group or candidate in a partisan race, even if the content of the action is not about those entities.

! The above information doesn't cover every situation. If in doubt, consult your command's ethics counselor.

APPENDIX

Online Conduct

The Navy defines online conduct as the use of electronic communications in an official or personal capacity, consistent with Navy values and standards of conduct. It is important that all Sailors and Navy civilians know when they are online they still represent the U.S. Navy.

Online bullying, hazing, harassment, stalking, discrimination, retaliation, and any other type of behavior that undermines dignity and respect are not consistent with Navy core values and negatively impact the force.

When conducting themselves online to include social media, Sailors and Navy civilians should:

- Consider what messages are being communicated and how they could be received
- Create or share content that is consistent with Navy values
- Only post if messages or content demonstrate dignity and respect for self and others

Deputy Secretary of Defense Policy Memorandum, Hazing and Bullying Prevention and Response in the Armed Forces, December 23, 2015, identifies hazing as so-called initiations or rites of passage in which individuals are subjected to physical or psychological harm. It identifies bullying as, "acts of aggression intended to single out individuals from their teammates or coworkers, or to exclude them from a military element, unit or Department of Defense organization." Additionally, the memo states that hazing and bullying are unacceptable and are prohibited in all circumstances and environments, including off duty or unofficial unit functions and settings, as well as on social media and other digital environments.

Also, intimate images taken without consent, or posted online without consent may constitute violations of the Uniform Code of Military Justice and Navy Regulations.

As outlined in the *CNO's Design for Maintaining Maritime Superiority* core attributes, the Navy is a values-based organization where everyone is expected to conduct themselves in a manner that is, "always upright and honorable, both in public or when no one is looking."

Joining Networks

Social media can be a positive tool for helping people with similar interests connect and interact. Sailors and Navy civilians should take care to ensure they are not participating in online or social media groups that do not reflect Navy core values, including groups that post graphic, obscene, explicit or racial comments, or groups posting comments that are abusive, hateful and vindictive, or intended to defame anyone or any organization.

Setting Guidelines

Leaders should communicate social media expectations with their Sailors and Navy civilians. It is important to outline policy, making sure Sailors and Navy civilians know what they can and cannot do on social media and other online platforms.

The UCMJ and Navy Regulations

When online, to include social media, Sailors are subject to the UCMJ and Navy Regulations, even when off duty. Commenting, posting or linking to material that violates the UCMJ or Navy Regulations may result in administrative or disciplinary action, to include administrative separation, and may subject civilians to appropriate disciplinary action.

Punitive action may include *Articles 88, 89, 91, 92, 120b*, *120c*, *133 or 134* (General Article provisions, Contempt, Disrespect, Insubordination, Indecent Language, Communicating a threat, Solicitation to commit another Offense, and Child Pornography offenses), as well as other articles, including Navy Regulations *Article 1168*, nonconsensual distribution or broadcast of an image.

Behaviors with Legal Consequences

Electronic harassment

47 U.S.C. § 223 (a)(1)(C) makes it a crime to anonymously use a telecommunications device (i.e. telephone, computer, or other electronic device used for communication) to harass a person; *47 U.S.C § 223 (a)(1)(E)* prohibits initiating communications via a telecommunications device solely to harass the recipient.

Electronic threats

18 U.S.C § 875 prohibits transmitting communications containing threats to kidnap or physically injure someone. It also criminalizes the actions of someone who, with intent to export (receive anything of value), electronically threatens to injure the property or reputation of a person. "Sextortion" (being tricked into providing sexual images and then being asked for money to not have the images published online) may fall under provisions of this law.

Cyber stalking

18 U.S.C. § 2261A prohibits a person, with the intent to kill, injure, harass, or intimidate someone, from using a computer (or other digital communications system), to engage in actions (course of conduct) reasonably expected to cause a person (or immediate family member, spouse, or intimate partner) substantial emotional distress.

Obscenity

47 U.S.C. § 223(a)(1)(A) prohibits using a telecommunications device to make, create, or solicit, and transmit any obscene comment, request, suggestion, proposal, image, or other communication.

Child exploitation / Child sexual exploitation

18 U.S.C. § 2251, *2252*, and *2252A*. Using a computer (a smartphone is a "computer") to solicit, make, create, transmit, or receive child pornography is illegal. For these provisions, a "child" is anyone under the age of 18. *18 U.S.C. § 1462* makes it a crime to transmit obscene matters. *18 U.S.C. § 1470* criminalizes the transfer of obscene materials, to include digital images, to persons under the age of 16. Sending sexually explicit (graphic "dirty" talk) electronic messages to minors, or soliciting sexually explicit communications, also are criminal offenses.

Computer misuse ("hacking")

A person engaging in cyber misconduct may also commit violations of *18 U.S.C. § 1030*, if, for example, he or she exceeds authorized access to the computer or accesses the computer without authorization (i.e. hacks into an account or network) to send the harassing, intimidating, humiliating, or even threatening communication.

Reporting Incidents

Any member of the Navy community who experiences or witnesses incidents of improper online behavior should promptly report it to their chain of command via the Command Managed Equal Opportunity manager or Fleet and Family Support office. Additional avenues for reporting include Equal Employment Opportunity offices, the Inspector General, Sexual Assault Prevention and Response offices and 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.

Specific instructions are available at *http://www.ncis.navy.mil/pages/NCISTips.aspx*.

Bottom Line

"Toxic behaviors...at work, at home, or on the internet – eat away at team cohesion and erode trust. Toxic behaviors cause us to hesitate, to second guess, to look over our shoulders instead of moving together at full speed. Toxic behaviors make us weaker; they cede advantage to the enemy. Toxic behaviors are NOT for winners, they are for losers. They have no place in our Navy."

Chief of Naval Operations Adm. John Richardson

Online Safety and Best Practices

There are a lot of reasons to go online: research, entertainment, chat, shopping, games, etc. While online, there are best practices that will help prevent the compromise of personal information and reputation. What happens online stays online and can have real-world impacts on a Sailor or Navy civilian where they work, at home, and with friends and loved ones years after.

Rules of the road for our Sailors and Navy civilians online:

When you are online, you are 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 is no such thing as complete anonymity online.

- "My user name is B@stSailrEvr, no one will figure out who I am." Wrong, the people you know will recognize you. And Google, Amazon and other online services that are designed to capture your online habits to optimize your experience will recognize you.

! **Online habits leave digital footprints.**

Before you hit send, stop and think ...

- Words and 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 can see what you post.

... the internet doesn't forget.

- It is 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 is best left unsaid, do not 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.
- And 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.

Security

When online, at work or afterhours, know how to protect yourself and the Navy. There are countries, criminals and hackers that are actively going after you as a Sailor and Navy civilian. Some are trying to get information from you and damage the Navy's networks; some are trying to get information about you so they can steal your identity and attack you personally, financially, or worse. They are looking for the weakest link in the online environment.

How to be a hard target:

- 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.
- Beware of tracking your location. Many social media platforms allow for "check in" and broadcast your location, or automatically add location information to photos and posts.
- Stay away from public Wi-Fi. With a public internet connection, you run the risk of being hacked. If you must use a public Wi-Fi connection, there 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 is a service you pay for that gives you a secure connection wherever you are.
    - 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.
    - 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.

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.
- Do not share passwords.
- Don't use the same password for more than one site or device.
- Never reuse an old password.
- 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. 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.
- 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.

AMERICA'S NAVY™

FORGED BY THE SEA