U.S. NAVY SOCIAL MEDIA HANDBOOK

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

PREPARED AND PRESENTED BY

NAVY OFFICE OF INFORMATION

FOR OFFICIAL USE ONLY

TABLE OF CONTENTS

INTRODUCTION

Social media has revolutionized our lives, from the way we communicate and interact with the world to the content we consume 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.

Millennials and Gen Z are the first "digital natives," meaning most have never known a world where instant information was not at their fingertips. While platform usage varies based on age, gender, race and ethnicity, one thing is certain – people today expect to have trusted, reliable and easily discoverable information at their fingertips. As an organization, we must balance the need for transparency and accuracy with today's known foreign malign influences – those who actively seek to spread misinformation and disinformation.

Social media, when used effectively, 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. The best social media strategies facilitate the free flow of information while preserving security, respecting privacy, and maintaining proper online conduct.

Careful decisions on the best platforms to use will ensure you convey the most relevant information as platforms rapidly adapt, age-out or emerge. Each section of this handbook is tailored to the unique audience it's serving: Navy leaders, communicators, Sailors, families, ombudsmen and civilians.

The U.S. Navy social media handbook covers many topics to assist the Navy family – whether a member of leadership, a Navy spouse or a member of the PA team – in effectively creating and maintaining your online presence. 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 NavySM@us.navy.mil.

LEADERS

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

Social media, when used effectively, presents significant opportunities to share the Navy story in an authentic, transparent and rapid manner while building richer, more substantive relationships with people the Navy may not reach through traditional communication channels.

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

Online Landscape

People use social media 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 communication objectives and that its targeted audiences use regularly.

It is important to remember that 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. If you decide social media would benefit your command, evaluate each platform to determine where your efforts will have the most impact; you don't need to use every platform.

Operational 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 we do as a Navy, social media can present OPSEC risks and challenges, but they can be mitigated. Manage 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 don't 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 your Sailors, Navy civilians and families post about themselves, including names, addresses, birthdates, birthplaces, local towns, schools, etc. It's important to remember small details can be aggregated to reveal significant information that could pose a threat. 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.

Foreign Malign Influence

Foreign malign influence (FMI) refers to efforts by foreign actors—state or non-state entities—to manipulate public opinion, spread disinformation, or undermine trust in institutions, typically to advance their own objectives.

A command's social media presence can be targeted by FMI in several ways, highlighting the importance of vigilance in how these platforms are managed.

- A command's social media channels are highly visible and accessible, making them a potential target for foreign actors seeking to exploit information. Adversaries may attempt to manipulate conversations, create fake accounts, or distort messages shared by the command, aiming to erode trust in the Navy and its leadership.

- Foreign malign actors often spread false narratives or misleading information, sometimes using a command's social media presence (comments section) to amplify these messages. This can confuse audiences, distort the Navy's narrative, and potentially cause reputational damage.

- If not properly managed, the spread of foreign disinformation or manipulation on a command's social media can negatively affect internal and external communication efforts. It may distract leaders from their primary goals and require additional resources to counter misinformation, affecting overall mission readiness and public trust.

- To counter FMI, remain vigilant in the management of all official social media accounts. Also ensure the social media content plan developed by public affairs staff aligns with Navy communication priorities, adheres to social media policy, protects OPSEC.

Fake Pages

Who creates them? Typically, actors aiming to undermine Navy credibility impersonate official organizational pages on social media.

What to do:

- Verify official pages: Have official command pages verified to establish credibility with platform users. Contact CHINFO at NavySM@us.navy.mil to have official pages verified; CHINFO will assist with the process.

- Report fake pages:

    - Platform: Use the social media platform's reporting tool.
    - CHINFO: Email links of fake pages to NavySM@us.navy.mil.

Political Activity

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 the Sailor's 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.

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.

Standards for Online Conduct

As a Navy leader, you must lead by example. You must show your Sailors and Navy civilians that improper or inappropriate 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 from 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 (UCMJ) or civil law by one of your Sailors or Navy civilians comes to your attention from social media, then you can act on it just as if it were witnessed in any other public location. Additionally, pursuant to Navy regulations, you have an affirmative obligation to act on UCMJ offenses you observe. This adds an ethical wrinkle to friending or following your subordinates; the key is for you to maintain the same relationship with them online as you do at work and to be clear about that.

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 being found in violation of UCMJ Articles 88, 89, 91, 92, 120b, 120c, 133 or 134 (General Article provisions for 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.

Reporting Incidents

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

Reports can be made to the 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 the Naval Criminal Investigative Service (NCIS).

NCIS encourages anyone with knowledge of criminal activity to report it to his or her local NCIS field office directly or via web or smartphone app.

Resources

All resources are available at www.navy.mil/SocialMedia.

1. **Social Media DoD Instruction 5400.17** – Covers DoD requirements for managing official social media.
2. **Navy Social Media Handbook** – A Navy guide on social media to support commands, Sailors and families.
3. **Navy Social Media Instructional Videos** – Videos covering social media best practices, identity management, and DoD policy.
4. **Social Media Guide for Leaders** – a one-page summary outlining important considerations about social media for Navy leaders.

COMMUNICATORS

To be the most effective communicators, we must build communication strategies that utilize platforms expertly – connecting desired outcomes with the target audiences. In order to create a successful online presence, ensure you understand the social landscape, your efforts align with your command's goals and objectives and that your team has the bandwidth to execute.

It's important to remember that 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.

If you decide social media would benefit your command, evaluate each platform to determine where your efforts will have the most impact. Don't 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.

Your content — stories, photos, videos (b-roll and productions), infographics (still and video), blogs, etc. — is needed to tell the Navy story. Follow current instructions on release of visual information and records management. Navy social media sites are official representations of the Department of the Navy and must demonstrate professionalism at all times. While third-party sites such as Facebook and X are not owned by the Navy, there are guidelines for the management of official Navy social media accounts.

Policy

DoD: Department of Defense (DoD) Instruction 5400.17 provides core principles regarding social media use within DoD. Additionally, DoDI 5400.17 and provides guidance regarding records management procedures for social media accounts and guidance on personal social media use by DoD personnel

Navy: SECNAVINST 5720.44C is the Department of the Navy Public Affairs Policy & Regulations. It 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 internet-based capabilities in writing. The administrator is responsible for ensuring postings to the webpages and social media platforms 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 Navy's current social media user agreement is required.

- LOCAL PROCEDURES: Commands and activities must develop written local procedures for the approval and release of all information posted on official command social media pages and websites.

- SECURITY: Commands will actively monitor and evaluate official websites and social media pages for compliance with security requirements and for fraudulent or unacceptable use.

- PRIMARY WEB PRESENCE: An official social media presence, including a blog platform, may not serve as the Navy entity's primary web presence and must link to the primary web presence, i.e., the command or activity's official website.

- PROHIBITED CONTENT: Commands and activities shall not publish and shall prohibit content such as: Personal attacks; vulgar, hateful, violent or racist language; slurs, stereotyping, hate speech, and other forms of discrimination based on any race, color, religion, national origin, disability or sexual orientation. Commands and activities must also prohibit information that may engender threats to the security of Navy and Navy operations or assets or to the safety of personnel and their families.

- CORRECTIONS TO PREVIOUS POSTS: If correcting a previous post by another contributor on an official page, such posting must be 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 your command's communication needs. Not every command needs a social media presence. It's far better to not start a social media site than to use it ineffectively and/or abandon the page later.

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

You also should consider your command's priority 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 military 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.

Alternatives

If your command wants to share information or content privately, social media is not your solution. Social media is never the right venue for sharing sensitive information.

- If you have sensitive information you want to limit to a specific group, consider one of the 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 public affairs officer and/or the Navy region PAO.

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

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

Strategy Development and Content Planning

Social media is not a substitute for a public affairs program. As you decide how social media can support it, consider your audience(s), goal, objectives and assessment method.

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.

Once released, all Navy content is in the public domain and may not include any copyrighted material such as music, photos, videos or graphics without the appropriate licensing.

In addition to deciding what you'll create, discuss when and where you'll share it. Not all your content needs to be shared at once or on all your sites. For example, content shared on the Navy's X account is frequently not shared on Facebook and vice versa. The X 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 X is about what's happening in the moment, content is tweeted more often than posted on Facebook.

Commands are responsible for official content posted on their social media pages. 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 before a contractor posts it.

Social Listening

An important part of a social media strategy is keeping track of what's being said about your command and understanding the significance of specific social conversations. Social listening is different from social monitoring. Listening involves both tracking mentions of a specific topic and extracting insights relevant to your strategy. Listening can reveal sentiment and trends.

A lot is happening all the time, and it's hard to keep up without diligently monitoring. CHINFO has several established streams checked throughout the day. Set up the following streams for you and your team to monitor daily:

- Mentions of account handles (e.g., @USNavy)
- Retweets
- Keywords associated with a command. For instance, not everyone uses the Navy handle (@USNavy), so it is also important to search for mentions of Navy, USNavy, #USNavy and U.S. Navy.
- Campaign or incident-specific keyword searches (e.g., "Navy + #AUKUS")

Assessments

To ensure social media efforts are achieving intended aims, communicators should conduct periodic assessments. Each social media site provides in-platform analytics. Tracking analytics weekly or monthly will reveal what type of content performs best. In addition to the keeping track of the size of your audience, it's important to see what content has the greatest reach and receives the most engagement from followers.

Assessments are also useful to evaluate one-off events and demonstrate to leadership the importance of social media for communicating Navy messaging. Recent examples are frequently shared in CHINFO's Playbooks and Sailing Directions, but reach out to the team if you need something specific to help you get started.

Influencers

Social media influencers are online content generators with large followings. Influencers may sometimes include Navy Sailors who generate social media content in a personal capacity while off duty. Always consult CHINFO (NavySM@us.navy.mil) prior to considering a social media influencer collaboration and ensure your command leadership reviews and approves the effort as well. Public affairs professionals at CHINFO will carefully vet influencers and ensure the command's potential collaboration will not negatively reflect on the command or Navy. Influencers can be effective in amplifying command messages and sharing the Navy story with broader audiences.

Adverse Incidents

Commands should leverage existing social media presences during a crisis, when appropriate. If you have a regularly updated channel of communication before a crisis, then your audiences will know where to find information online.

Don't make your audience search for information. For example, if your command is preparing for severe weather, tell your audience where they should go for the latest information.

Casualties

When personnel are killed, wounded or missing in action, social media can play a role (good or bad). Media may look at command, Sailor, Navy civilian and family members' social media pages to obtain information.

It is vitally important that all Sailors, Navy civilians, family members and friends know that the identity of a casualty should not be discussed on social media until it has been formally released. In accordance with Department of Defense (DoD) Instruction 1300.18, 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.

When a crisis occurs, work with the full Navy PA team to identify and direct people to the appropriate spokesperson and online source of information. This will help minimize misinformation.

Foreign Malign Influence

Foreign malign influence (FMI) refers to efforts by foreign actors—state or non-state entities—to manipulate public opinion, spread disinformation, or undermine trust in institutions, typically to advance their own objectives.

A command's social media presence can be targeted by FMI in several ways, highlighting the importance of vigilance in how these platforms are managed.

- A command's social media channels are highly visible and accessible, making them a potential target for foreign actors seeking to exploit information. Adversaries may attempt to manipulate conversations, create fake accounts, or distort messages shared by the command, aiming to erode trust in the Navy and its leadership.

- Foreign malign actors often spread false narratives or misleading information, sometimes using a command's social media presence (comments section) to amplify these messages. This can confuse audiences, distort the Navy's narrative, and potentially cause reputational damage.

- If not properly managed, the spread of foreign disinformation or manipulation on a command's social media can negatively affect internal and external communication efforts. It may distract leaders from their primary goals and require additional resources to counter misinformation, affecting overall mission readiness and public trust.

To counter FMI, remain vigilant in the management of all official social media accounts. Also ensure the social media content plan developed by public affairs staff aligns with Navy communication priorities, adheres to social media policy, protects OPSEC.

Political Activity 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 online 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 judge advocate general or contracting officer for exceptions and additional information.

Operational Security (OPSEC)

Social media amplifies OPSEC risks because it enables a greater volume of information to be rapidly shared publicly. Navy communicators should carefully consider the level of detail included when posting information anywhere on the internet, and they should err on the side of caution.

Local procedures should be established to ensure all information posted on social media is releasable and in accordance with local public affairs guidance and Navy Public Affairs regulations. It is the responsibility of the social media managers to identify and remove information that may compromise OPSEC.

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

- DEPLOYMENT: You should minimize the risk of sharing information related to a current deployment. Instead of saying the "Sailor is in ABC unit at DEF camp in GHI city in Afghanistan," it can be rephrased to the "Sailor is deployed." Close family and friends should already know additional details if allowed, so there's no need to post more specifics online. Assume that anyone can see any information posted and shared.

- SCHEDULES: Posts about scheduled movements and current or future locations should be avoided. Generally, it's safer to talk about events that have happened rather than what will happen — unless that information has been formally released by the Navy to the public.

- PERSONAL INFORMATION: Avoid posting personal information such as deployment status, addresses, telephone numbers, location information, schedules, family member information (e.g., names, addresses, birthdates, birthplaces, local towns, schools), etc.

- 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 who they claim to be. Be mindful of others attempting to use social presences as a means of targeting individuals. Only establish and maintain connections with people who are known and trusted. Review your connections often.

Other information that should not be shared includes descriptions of military facilities, unit morale, future operations or plans, results of operations, technical information, details of weapons systems and equipment status, as well as the discussion of daily routines and frequently visited locations.

Communicators are encouraged to post about pride and support for teammates and units, general insights about service or duty, port call information after the Navy has released it to the public; general status of the location of a ship at sea (e.g., operating in the Pacific Ocean, as opposed to off the coast of San Diego) in coordination with public affairs staff; 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's important and what they can do if they think they know of a violation.

Fake Pages

Who creates them? Typically, actors aiming to undermine Navy credibility impersonate official organizational pages on social media.

What to do:

- Verify official pages: Have official command pages verified to establish credibility with platform users. Contact CHINFO at NavySM@us.navy.mil to have official pages verified; CHINFO will assist with the process.

- Report fake pages:
  - Platform: Use the social media platform's reporting tool.
  - CHINFO: Email links of fake pages to NavySM@us.navy.mil.

Blocking and Removing Content

The Navy may not block individual social media accounts from official Navy social media sites. However, the Navy may delete comments that constitute a violation of law, regulation, or the Navy's terms of use. The Navy may also refer offensive comments to the social media service provider to consider enforcement of their own terms of service.

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

Comments posted on official Navy social media sites that constitute a violation of law, regulation or the Navy's terms of use may be removed if not needed for evidentiary purposes.

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

Comments posted on official Navy social media sites that constitute a violation of the terms of service of the social media service provider may be referred to the service provider for their own review and possible enforcement of the terms of service.

Reporting Improper 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 the Naval Criminal Investigative Service.

NCIS encourages anyone with knowledge of criminal activity to report it to their local NCIS field office directly or via web or smartphone app.

Resources

All resources are available at www.navy.mil/SocialMedia.

1. **Social Media DoD Instruction 5400.17** – Covers DoD requirements for managing official social media.

2. **Navy Social Media Handbook** – A Navy guide on social media to support commands, Sailors and families.

3.**Navy Social Media Instructional Videos** – Videos covering social media best practices, identity management, and DoD policy.

4. **Social Media Guide for Leaders** – a one-page summary outlining important considerations about social media for Navy leaders.

5. **How-To Guides** – Links to online instructions for creating and managing accounts on social media platforms.

SAILORS

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

It's never been easier for a Sailor to reach a large, public audience intentionally or unintentionally through email, social media, blogs and other platforms. While most Sailors neither work in public affairs nor officially speak on behalf of the Navy, all Sailors must recognize that they may be perceived as a spokesperson for the Navy simply because they wear a Navy uniform.

As a Sailor, you are sometimes the Navy's most effective representative. You can share a direct, unfiltered perception of what it means to serve your country and can provide personal insights into Navy life. 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 outlines best practices you should follow while using social media.

Online Conduct

It's often hard to distinguish between personal or professional representation on the internet, so Sailors should assume any content posted could affect their Navy career and the reputation of the Navy more broadly. Sailors should not engage in any conversations or activities that are contrary to the Navy's core values or could potentially jeopardize operational readiness.

Content that is defamatory, threatening, harassing, or discriminatory on the basis of race, color, sex, gender, age, religion, national origin, sexual orientation or any other protected status is prohibited and punishable and should therefore be avoided. The internet doesn't forget; online habits leave digital footprints. Be cautious when posting content, even if your post is intended for a private audience.

Operational Security (OPSEC)

Social media amplifies OPSEC risks because it enables a greater volume of information to be rapidly shared publicly. Sailors should carefully consider the level of detail included when posting information anywhere on the internet, and they should err on the side of caution. "Loose Lips Sink Ships," so practice good OPSEC at all times.

OPSEC best practices:

- DEPLOYMENT: You should minimize the risk of sharing information related to a current deployment. Instead of saying "I am in ABC unit at DEF camp in GHI city in Afghanistan," it can be rephrased to "I am deployed." Close family and friends should already know additional details if allowed, so there's no need to post more specifics online. Assume that anyone can see any information posted and shared.

- SCHEDULES: Posts about scheduled movements and current or future locations should be avoided. Generally, it's safer to talk about events that have happened rather than what will happen — unless that information has been formally released by the Navy to the public.

- PERSONAL INFORMATION: Avoid posting personal information such as deployment status, addresses, telephone numbers, location information, schedules, family member information (e.g., names, addresses, birthdates, birthplaces, local towns, schools), etc.

- 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 who they claim to be. Be mindful of others attempting to use social presences as a means of targeting individuals. Only establish and maintain connections with people who are known and trusted. Review your connections often.

Other information that should not be shared includes descriptions of military facilities, unit morale, future operations or plans, results of operations, technical information, details of weapons systems and equipment status, as well as the discussion of daily routines and frequently visited locations.

Sailors are encouraged to post about pride and support for teammates and units, general insights about service or duty, port call information after the Navy has released it to the public, and content from official Navy social media sites.

Uniform Code of Military Justice (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 being found in violation of UCMJ Articles 88, 89, 91, 92, 120b, 120c, 133 or 134 (General Article provisions for 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 potential legal consequences include:
- Child exploitation/Child sexual exploitation
- Computer misuse (hacking)
- Cyber stalking
- Electronic harassment
- Electronic threats
- Obscenity

Cyberbullying

While social media sites allow people to connect with loved ones and friends, they can also enable bullying and harassment.

According to a study conducted in 2018 by Pew Research Center, 59% of teens in the U.S. have personally experienced abusive behavior online. The most common type of harassment teens encounter online is name-calling (42%). About a third (32%) of teens say that someone has spread false rumors about them online; while 21% have had someone other than a parent constantly ask where they are, who they are with or what they are doing; and 16% have been the target of physical threats online.

Online bullying, hazing, harassment, stalking, discrimination, retaliation, and any other type of behavior that undermines dignity and respect are inconsistent with Navy core values and therefore negatively impact the force. Any member of the Navy community experiencing or witnessing incidents of improper online behavior by a Navy community member should report the activity to their chain of command via the Command Managed Equal Opportunity (CMEO) or Fleet and Family Support Office.

You can also report a user, message or post in-platform. Facebook, X and Instagram all provide the option of blocking a user. On Facebook, you can report an individual post or comment by selecting "Give feedback on this post" in the upper right-hand corner of a post or "Give feedback or report this comment" next to a comment. You can report a tweet by clicking the downward arrow icon and selecting "Report Tweet." On Instagram, you can report a post by selecting "Report" in the upper right-hand corner. If someone leaves an inappropriate comment on your Facebook or Instagram post, you can delete it.

Sailors should engage in respectful conduct on social media and report improper online behavior.

Cybersecurity

Social media sites can open users and their systems to security weaknesses. Remember, hacking, configuration errors, social engineering and the sale/sharing of user data mean your information could become public at any time.

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, 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 WiFi hotspots).

Private Groups

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

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. Additionally, you must never solicit gifts or prizes for command events in any capacity — on duty, off duty or in a personal capacity.

Political Activity

Active-duty Sailors may generally express personal views about public issues or political candidates using social media — just like they can write a letter to a newspaper 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 (on duty or while in uniform) may not engage in partisan political activity, such as posting direct links to a political party, partisan political candidate, campaign, group or cause. Additionally, distributing literature on behalf of partisan entities or individuals is prohibited.

Active-duty Sailors can like, share or follow social media posts from 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 UCMJ and rules about the use of government resources and government communications systems, including email and internet.

Adverse Incidents

Social media is a major part of most people's lives during good times and bad times. When our teammates are killed, wounded or missing in action, it is hard to control the flow of information distributed through social media platforms. However, it important to approach such situations with great caution and keep in mind the privacy considerations and sensitivities of friends and loved ones.

In accordance with Department of Defense (DoD) Instruction 1300.18, 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.

General guidelines:

- Consult Navy public affairs staff before posting.
- Always follow unit protocol and don't add to rumors and speculation.
- If approached by someone online, state that you do not know and they should not speculate.
- If approached by a member of the media, simply refer them to Navy public affairs staff.

Reporting Improper 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 the Naval Criminal Investigative Service.

NCIS encourages anyone with knowledge of criminal activity to report it to their local NCIS field office directly or via web or smartphone app.

Resources

All resources are available at www.navy.mil/SocialMedia.

1. **Social Media DoD Instruction 5400.17** – Covers DoD requirements for managing official social media.

2. **Navy Social Media Handbook** – A Navy guide on social media to support commands, Sailors and families.

3. **Navy Social Media Instructional Videos** – Videos covering social media best practices, identity management, and DoD policy.

4. **Social Media Guide for Leaders** – a one-page summary outlining important considerations about social media for Navy leaders.

5. **How-To Guides** – Links to online instructions for creating and managing accounts on social media platforms.

FAMILIES

We're grateful for the dedicated support of our Navy families. One way for families to support their Sailor is to share the Navy story — responsibly.

Strong, capable families enable Sailors to remain prepared in defending freedom and protecting our nation's interests abroad. Because families are such a big part of our Navy, it is crucial that they share their stories while following important guidelines to preserve OPSEC and propriety. This section addresses best practices for Navy families on social media.

Operational Security (OPSEC)

Social media amplifies OPSEC risks because it enables a greater volume of information to be rapidly shared publicly. Families should be especially careful when discussing their Sailor's current deployments, scheduled ship 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," it is better to say, "My Sailor is deployed in the Pacific.
- Instead of saying, "My Sailor will be back in 53 days" it is better to say "My Sailor is coming home."
- Thoughtfully consider the level of detail included when posting information anywhere on the internet, and err on the side of caution.
- SCHEDULES: Posts about scheduled movements and current or future locations should be avoided. Generally, it's safer to talk about events that have happened rather than what will happen — unless that information has been formally released by the Navy to the public.
- PERSONAL INFORMATION: Avoid posting personal information such as deployment status, addresses, telephone numbers, location information, schedules, family member information (e.g., names, addresses, birthdates, birthplaces, local towns, schools), etc.
- 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 who they claim to be. Be mindful of others attempting to use social presences as a means of targeting individuals. Only establish and maintain connections with people who are known and trusted. Review your connections often.

Social Media Post Examples	
Bad Post	**Good Post**
1. My son, IT2 Any Sailor, is in Any Unit at Naval Station Anywhere in Any City, Japan 2. My daugher Lt. Any Sailor, is aboard USS John C. Stennis. She's coming home in 53 days. 3. My family is in Houston, Texas	1. My Sailor is deployed in the Pacific. 2. My daughter's ship is coming home soon. 3. My family is from Texas

Cybersecurity

Social media sites can open users and their systems to security weaknesses. Remember, hacking, configuration errors, social engineering and the sale/sharing of user data mean your information could become public at any time.

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, 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 WiFi hotspots).

Cyberbullying

While social media sites allow people to connect with loved ones and friends, they can also enable bullying and harassment.

According to a study conducted in 2018 by Pew Research Center, 59% of teens in the U.S. have personally experienced abusive behavior online. The most common type of harassment teens encounter online is name-calling (42%). About a third (32%) of teens say that someone has spread false rumors about them online; while 21% have had someone other than a parent constantly ask where they are, who they are with or what they are doing; and 16% have been the target of physical threats online.

Online bullying, hazing, harassment, stalking, discrimination, retaliation, and any other type of behavior that undermines dignity and respect are inconsistent with Navy core values and therefore negatively impact the force. Any member of the Navy community experiencing or witnessing incidents of improper online behavior by a Navy community member should report the activity to their chain of command via the Command Managed Equal Opportunity (CMEO) or Fleet and Family Support Office.

You can also report a user, message or post in-platform. Facebook, X and Instagram all provide the option of blocking a user. On Facebook, you can report an individual post or comment by selecting “Give feedback on this post” in the upper right-hand corner of a post or “Give feedback or report this comment” next to a comment. You can report a tweet by clicking the downward arrow icon and selecting “Report Tweet.” On Instagram, you can report a post by selecting “Report” in the upper right-hand corner. If someone leaves an inappropriate comment on your Facebook or Instagram post, you can delete it.

Adverse Incidents

Social media is a major part of most people’s lives during good times and bad times. When our teammates are killed, wounded or missing in action, it is hard to control the flow of information distributed through social media platforms. However, it important to approach such situations with great caution and keep in mind the privacy considerations and sensitivities of friends and loved ones.

In accordance with Department of Defense (DoD) Instruction 1300.18, 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.

Recommendations:

- Consult Navy public affairs staff before posting.
- Always follow unit protocol and don't add to rumors and speculation.
- If approached by someone online, state that you do not know and they should not speculate.
- If approached by a member of the media, simply refer them to Navy public affairs staff.

Resources

All resources are available at www.navy.mil/SocialMedia.

1. **Navy Social Media Handbook** – A Navy guide on social media to support commands, Sailors and families.

2. **Navy Social Media Instructional Videos** – Videos covering social media best practices, identity management, and DoD policy.

3. **How-To Guides** – Links to online instructions for creating and managing accounts on social media platforms.

OMBUDSMEN

The Navy has an obligation to provide timely and accurate information to the public; keep Sailors, Navy civilians, and their families informed; and build relationships with local communities. Ombudsmen take on a vital role in this process, serving as a critical link between the command leadership and Navy families.

Navy families often look to command ombudsmen for official information on their Sailor or unit, particularly during deployment. Because families are such a big part of our Navy, it is crucial that ombudsmen are equipped with best practices for sharing relevant information with Navy families while following important guidelines to preserve OPSEC and propriety. This section addresses best practices for Navy ombudsmen on social media.

Supporting Command Social Media

When ships or units are deployed, they have less bandwidth or no internet connection at all, which makes it difficult to update social media sites. Having someone shoreside to help post released updates, photos and videos can be extremely helpful. We recommend that ombudsmen talk to the public affairs staff and/or command leadership before deployment and discuss how ombudsmen can help. 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. Ombudsmen are in an excellent position to encourage discussion. People will be honest, ask questions, and express concerns, and the feedback enables command leadership to address them.

Active ombudsman participation is critical for supporting family readiness through social media. A well-coordinated command social media presence, with active participation from an ombudsmen and command leadership, presents a cohesive and supportive environment that leads to better communication and stronger family readiness.

Many commands have unofficial social media presences established by former crew members, veterans or supporters excited about the command. Ombudsmen should work with command leadership to determine if they want to simply monitor the unofficial and/or chime in when they have information to add. Ombudsmen may want to contact the administrator to see how they can work together. Regardless, this should not stop ombudsmen or the command from creating an official presence for the command and its families.

Official presences are listed in the Navy Social Media Directory (listing only command presences, not family readiness groups), which can be found at www.navy.mil/socialmedia. If you find an online presence portraying itself as an official presence and the command is not sponsoring it, the command public affairs staff should contact the Navy Office of Information at NavySM@us.navy.mil.

When turning over ombudsman duties, the outgoing ombudsman should teach the incoming ombudsman how the social media account works and is used. Then, introduce the new ombudsman on the platform and send a sign-off message. The outgoing ombudsman may also recommend the new ombudsman post a photo and/or note introducing himself or herself. Finally, ensure the new ombudsman is made into an account administrator (Facebook) and/or provided the account's username and password.

Operational Security (OPSEC)

Social media amplifies OPSEC risks because it enables a greater volume of information to be rapidly shared publicly. Families should be especially careful when discussing their Sailor's current deployments, scheduled ship 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," it is better to say, "My Sailor is deployed in the Pacific.
- Instead of saying, "My Sailor will be back in 53 days" it is better to say "My Sailor is coming home."
- Thoughtfully consider the level of detail included when posting information anywhere on the internet, and err on the side of caution.
- SCHEDULES: Posts about scheduled movements and current or future locations should be avoided. Generally, it's safer to talk about events that have happened rather than what will happen — unless that information has been formally released by the Navy to the public.
- PERSONAL INFORMATION: Avoid posting personal information such as deployment status, addresses, telephone numbers, location information, schedules, family member information (e.g., names, addresses, birthdates, birthplaces, local towns, schools), etc.
- 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 who they claim to be. Be mindful of others attempting to use social presences as a means of targeting individuals. Only establish and maintain connections with people who are known and trusted. Review your connections often.
- Ombudsmen may find themselves educating Navy 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 don't 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.

Social Media Post Examples	
Bad Post	**Good Post**
1. My son, IT2 Any Sailor, is in Any Unit at Naval Station Anywhere in Any City, Japan 2. My daugher Lt. Any Sailor, is aboard USS John C. Stennis. She's coming home in 53 days. 3. My family is in Houston, Texas	1. My Sailor is deployed in the Pacific. 2. My daughter's ship is coming home soon. 3. My family is from Texas

Private Groups

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

Cybersecurity

Social media sites can open users and their systems to security weaknesses. Remember, hacking, configuration errors, social engineering and the sale/sharing of user data mean your information could become public at any time.

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, 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 WiFi hotspots).

Cyberbullying

While social media sites allow people to connect with loved ones and friends, they can also enable bullying and harassment.

According to a study conducted in 2018 by Pew Research Center, 59% of teens in the U.S. have personally experienced abusive behavior online. The most common type of harassment teens encounter online is name-calling (42%). About a third (32%) of teens say that someone has spread false rumors about them online; while 21% have had someone other than a parent constantly ask where they are, who they are with or what they are doing; and 16% have been the target of physical threats online.

Online bullying, hazing, harassment, stalking, discrimination, retaliation, and any other type of behavior that undermines dignity and respect are inconsistent with Navy core values and therefore negatively impact the force. Any member of the Navy community experiencing or witnessing incidents of improper online behavior by a Navy community member should report the activity to their chain of command via the Command Managed Equal Opportunity (CMEO) or Fleet and Family Support Office.

You can also report a user, message or post in-platform. Facebook, X and Instagram all provide the option of blocking a user. On Facebook, you can report an individual post or comment by selecting "Give feedback on this post" in the upper right-hand corner of a post or "Give feedback or report this comment" next to a comment. You can report a tweet by clicking the downward arrow icon and selecting "Report Tweet." On Instagram, you can report a post by selecting "Report" in the upper right-hand corner. If someone leaves an inappropriate comment on your Facebook or Instagram post, you can delete it.

Adverse Incidents

Social media is a major part of most people's lives during good times and bad times. When our teammates are killed, wounded or missing in action, it is hard to control the flow of information distributed through social media platforms. However, it important to approach such situations with great caution and keep in mind the privacy considerations and sensitivities of friends and loved ones.

In accordance with Department of Defense (DoD) Instruction 1300.18, 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.

Recommendations:

- Consult Navy public affairs staff before posting.
- Always follow unit protocol and don't add to rumors and speculation.
- If approached by someone online, state that you do not know and they should not speculate.
- If approached by a member of the media, simply refer them to Navy public affairs staff.

Resources

All resources are available at www.navy.mil/SocialMedia.

1. **Navy Social Media Handbook** – A Navy guide on social media to support commands, Sailors and families.

2. **Navy Social Media Instructional Videos** – Videos covering social media best practices, identity management, and DoD policy.

3. **How-To Guides** – Links to online instructions for creating and managing accounts on social media platforms.

NAVY CIVILIANS

Navy civilians play a key role in supporting the Navy mission around the world. Navy civilians serve as ambassadors of the Navy, and it is therefore important they understand what it means to communicate and represent the Navy responsibly online.

Navy civilians should recognize that they may be perceived as a Navy spokesperson simply by association. Therefore, Navy civilians must understand how to communicate responsibly and avoid doing or saying anything that could cast the Navy in a negative light.

This handbook offers key considerations and best practices for Navy civilians to follow while using social media.

Online Conduct

It's often hard to distinguish between personal or professional representation on the internet, so Navy civilians should assume any content posted could affect their Navy career and the reputation of the Navy more broadly. Navy civilians should not engage in any conversations or activities that are contrary to the Navy's core values or could potentially jeopardize operational readiness.

Content that is defamatory, threatening, harassing, or discriminatory on the basis of race, color, sex, gender, age, religion, national origin, sexual orientation or any other protected status should be avoided. The internet doesn't forget; online habits leave digital footprints. Be cautious when posting content, even if your post is intended for a private audience.

Operational Security (OPSEC)

Social media amplifies OPSEC risks because it enables a greater volume of information to be rapidly shared publicly. Navy civilians should carefully consider the level of detail included when posting information anywhere on the internet, and they should err on the side of caution. "Loose Lips Sink Ships," so practice good OPSEC at all times.

OPSEC best practices:

- SCHEDULES: Posts about scheduled movements and current or future locations should be avoided. Generally, it's safer to talk about events that have happened rather than what will happen — unless that information has been formally released by the Navy to the public.

- PERSONAL INFORMATION: Avoid posting personal information such as deployment status, addresses, telephone numbers, location information, schedules, family member information (e.g., names, addresses, birthdates, birthplaces, local towns, schools), etc.

- 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 who they claim to be. Be mindful of others attempting to use social presences as a means of targeting individuals. Only establish and maintain connections with people who are known and trusted. Review your connections often.

Other information that should not be shared includes descriptions of military facilities, unit morale, future operations or plans, results of operations, technical information, details of weapons systems and equipment status, as well as the discussion of daily routines and frequently visited locations.

Cyberbullying

While social media sites allow people to connect with loved ones and friends, they can also enable bullying and harassment.

According to a study conducted in 2018 by Pew Research Center, 59% of teens in the U.S. have personally experienced abusive behavior online. The most common type of harassment teens encounter online is name-calling (42%). About a third (32%) of teens say that someone has spread false rumors about them online; while 21% have had someone other than a parent constantly ask where they are, who they are with or what they are doing; and 16% have been the target of physical threats online.

Online bullying, hazing, harassment, stalking, discrimination, retaliation, and any other type of behavior that undermines dignity and respect are inconsistent with Navy core values and therefore negatively impact the force. Any member of the Navy community experiencing or witnessing incidents of improper online behavior by a Navy community member should report the activity to their chain of command via the Command Managed Equal Opportunity (CMEO) or Fleet and Family Support Office.

You can also report a user, message or post in-platform. Facebook, X and Instagram all provide the option of blocking a user. On Facebook, you can report an individual post or comment by selecting "Give feedback on this post" in the upper right-hand corner of a post or "Give feedback or report this comment" next to a comment. You can report a tweet by clicking the downward arrow icon and selecting "Report Tweet." On Instagram, you can report a post by selecting "Report" in the upper right-hand corner. If someone leaves an inappropriate comment on your Facebook or Instagram post, you can delete it.

Navy civilians should engage in respectful conduct on social media and report improper online behavior.

Cybersecurity

Social media sites can open users and their systems to security weaknesses. Remember, hacking, configuration errors, social engineering and the sale/sharing of user data mean your information could become public at any time.

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, 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 WiFi hotspots).

Political Activity

Before posting about politics on social media, Navy civilians should consider the Hatch Act and Department of Defense policy. In general, as a federal employee, you may use social media in compliance with the Hatch Act if you:

- Don't engage in political activity while "on duty" or in the workplace, even if you're 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 post political opinions, likes, shares, etc. while on government property, even if inside your vehicle on a lunch break, using your own device to post to your personal account.

- 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's 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.

- Posting political opinions/likes/shares while on government property, even if inside your vehicle on a lunch break, using your own device to post to your personal account.

Civilians who fall in the "further restricted employees" category may express 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 social media profiles, even if the profile also contains their official title or position, without more. Civilians may also display a political party or campaign logo or a candidate photograph in profile pictures, 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 partisan 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.

For the full policy and more details, see the U.S. Office of Special Counsel website.

Resources

All resources are available at www.navy.mil/SocialMedia.

1.**Social Media DoD Instruction 5400.17** – Covers DoD requirements for managing official social media.

2.**Navy Social Media Handbook** – A Navy guide on social media to support commands, Sailors and families.

3.**Navy Social Media Instructional Videos** – Videos covering social media best practices, identity management, and DoD policy.

4.**Social Media Guide for Leaders** – a one-page summary outlining important considerations about social media for Navy leaders.

5.**How-To Guides** – Links to online instructions for creating and managing accounts on social media platforms.