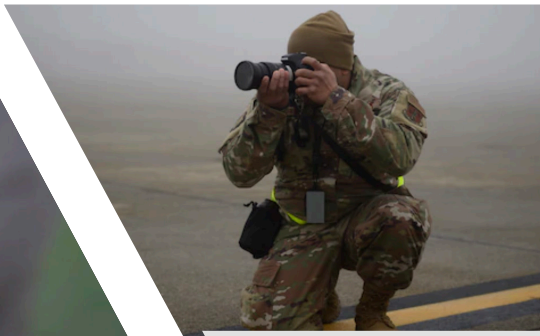
Social Media Guide

Department of the Air Force Public Affairs



Updated 6/2021

Table of Contents

4 Introduction

4 Social Media Overview

5 Is Social Media Right for Your Command?

6 Department of Defense and Department of the Air Force Policies

7 Visual Information

7 Registering Official Department of the Air Force Websites

7 Communication Planning

8 Strategy Development & Content Planning

9 Account Verification

9 Records Management

10 Branding Guidelines

11 Operations Security & Social Media

11 Security & Password Protection

13 Monitoring/Responding

13 Imposter/Fake Accounts

14 Bots

15 Crisis Communications

17 Correct the Record

17 Handling Social Media Mistakes

18 Alternatives to Social Media

18 Social Media & Your Command

19 Social Media Management Tools

20 Social Assessments

22 Metrics

Table of Contents (continued)

22 Key Performance Indicators (KPIs)

22 Online Advertising

23 Podcasts

24 Live Streaming

25 Guidelines for Airmen, Guardians, DAF Civilians & Families

- 25 Social Media & Leaders
- 25 Social Media & DAF Members
- 26 Social Media & DAF Families

27 Online Conduct

28 Political Activity

- 28 Airmen & Guardians
- 28 DAF Civilians
- 29 Politics & Social Media

29 Endorsements

30 Reporting Incidents

30 Cybersecurity

30 Cyberbullying

32 Contacts & Acknowledgements

33 Appendix A Social Media Account Verification Request Checklist

34 Appendix B Social Media Registry Checklist

35 Appendix C Tips to Stay Safe Online

37 Appendix D Reporting Social Media Comments of Concern

38 Appendix E Cyberbullying

39 Appendix F Air Force Podcast Production Workflow Checklist

Introduction

This guide will help you share information effectively while following Department of the Air Force instructions and protecting operational security. It is for informational purposes and does not replace official Department of the Air Force or Department of Defense policy.

People across all demographic categories use social media for differing purposes such as entertainment, networking and information source.

Social media, when used effectively, presents unequaled opportunities for you to share the stories of the Air and Space Forces in an authentic, transparent and rapid manner while building richer, more substantive relationships with people you may not have reached through traditional communication channels.

In the context of military activities and operations, the proper planning, execution and assessment of communication using social media provides a powerful tool for commanders. As a crucial enabler to the Air Force's Information Warfare (IW) capability, Public Affairs (PA) supports the employment of military capabilities in and through the information environment to affect adversary behavior and preserve friendly freedom of action. Through the informed release of accurate information through social media, official Air Force sources put activities and operations in contexts that facilitate informed perceptions about those operations; as well as counter misinformation, disinformation, propaganda and other forms of malign influence. Ultimately, these activities aid the understanding, trust and support of the U.S. population, allies and partners while also acting to deter, dissuade and otherwise influence adversaries.

Conversely, the open, global nature of social media creates challenges, including adversary IW, cybersecurity considerations and concerns regarding online conduct to include cyberbullying and harassment. Careful judgements about which platforms to use helps ensure we convey the most relevant information as platforms rapidly adapt, age-out or emerge.

Since social media is constantly evolving, this document presents enduring information that will remain relevant for some time. Frequently visit https://usaf.dps.mil/sites/10066/SitePages/Home.aspx for the latest policy, guidelines, best practices, standard operating procedures, training and other resources.

Social Media Overview

Social media is one of the primary modes of communication to the DAF's external publics (domestic and foreign). Use social media to tell the DAF story, but also to communicate during crises, engage with the media, and provide accurate and up-to-date information when news breaks. Today's world is connected 24/7. Social media is a key communication tool for listening and gaining important insight and perspective.

Is Social Media Right for Your 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 not to start a social media site than to use it ineffectively and abandon the site.

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 Airmen, Guardians, DAF 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 communication tool. If it isn't, take the opportunity to address the underlying issues using the best practices in this guide.

Remember, all social media sites require active oversight to ensure proper management. Take these commitments into account when weighing whether to create a new social media presence.

The following is a quick overview about what a few platforms do. You will need to determine which platform(s) will best serve your command's communication needs.

- Facebook—Facebook offers the most potential for engagement, so it's no wonder posts with questions or conversation starters perform the best. Try to start a conversation, which means listening even more than talking, with each post. Include questions as often as possible.
- Twitter—Bite-sized, repeatable phrases live here. You can discuss the same event in five different ways, and post them over the course of three days without boring followers with the information. Don't work too hard to seem cheeky, but this is the platform to stretch your witty legs and grab attention.
- Instagram—If you have an Instagram account, you're curating a lifestyle brand. Followers open Instagram, not to read the news, but to surround themselves with lifestyle images and verbiage, so use it to curate the brand you want Airmen to buy into and be proud of.

Department of Defense and Department of the Air Force Policies

The following Department of Defense and Department of the Air Force publications contain information to consider when using social media. DOD web policies are viewable at Chief Information Officer Web and Social Media Policies. DAF instructions are accessible at Department of the Air Force E-publishing.

- DODi 8170.01, *Online Information Management and Electronic Messaging* provides a compendium of policies and procedures critical to successful online information management and electronic messaging and establishes policy, assigns responsibilities and prescribes practices for:
    - Conducting, establishing, operating and maintaining electronic messaging services (including, but not limited to, e-mail) to collect, distribute, store, and otherwise process official DOD information, both unclassified and classified, as applicable.
    - Managing official DOD information on the DOD Information Network and other networks, i.e., online.
- The DOD Social Media Hub is designed to help the DOD community use social media and other Internet-based Capabilities (IbC) responsibly and effectively; both in official and unofficial (i.e., personal/private) capacities.
- Several Department of the Air Force instructions govern the use of social media. The decision to use a social media platform or tool (or combination of tools) must be based on a communications plan and must address the commitment of resources necessary to manage and maintain the public engagement. See the Air Force Web Policy page at https://www.af.mil/Web-Policy/.
- AFI 1-1, *Air Force Standards*, outlines how Airmen and Guardians should conduct themselves. Chapter 2.15. Use of Social Media specifically addresses social media sites.
- AFH 33-337, *Tongue and Quill*, together with AFMAN 33-326, *Preparing Official Communications*, provides the information to ensure clear communications—written or spoken.
- AFI 35-101, *Public Affairs Operations* provides guidance for conducting public affairs activities pertaining to general Public Affairs (PA) duties, responsibilities, and organization.
- Annex 3-61, *Public Affairs Operations*, from Air University, provides a broad doctrinal perspective on the employment of public affairs capabilities, such as social media, in an operational context, with discussion on the application of those capabilities in support of Operations in the Information Environment and Information Warfare.

Visual Information

The Department of the Air Force Visual Information (VI) mission is to gather, accession, maintain and archive VI as an irreplaceable account of Department of the Air Force activities. Department of the Air Force VI will be established in accordance with DoDI 5040.02, and DoDI 5040.07, *Visual Information (VI) Productions*. AFI 35-101, Chapter 7, *Visual Information*, defines the overall management of all DAF VI. These references are of particular relevance to using VI in social media activities:

- Section 7.7. *Authorized Use of Department of the Air Force VI Resources,* particularly 7.7.3. Imagery taken by Department of the Air Force personnel using personal cameras and equipment for non-official purposes will be considered personal imagery as long as it is not related to missions, operations, exercises and training (hereinafter "mission-related VI").
- Sections 7.8 *Quality Control* and 7.18 *Visual Information Production Management* are references for photo/video approval.

Registering Official Department of the Air Force Websites

Per DOD Web Policy, registration of all websites and social media accounts is required. Official social media accounts shall be registered via a service-specific registry. After a service has approved a site, it will be added to the main DOD registry.

All official DAF web presences (e.g. social media sites and official websites) should be registered at https://www.af.mil/AF-Sites/Site-Registration/. All submissions, if approved, will be added to the DAF social media registry.

Further, OMB Memo M-17-06, *Policies for Federal Agency Public Websites and Digital Services* states:
"To help confirm the validity of official U.S. Government digital platforms, within 60 days of the publication date of this Memorandum, agencies must register their public-facing digital services such as social media, collaboration accounts, mobile apps and mobile websites with the U.S. Digital Registry at: http://www.digitalgov.gov/services/u-s-digital-registry/.

Communication Planning

Before establishing official Air Force social media accounts, consider developing a plan for your commander about how each account could benefit your organization's communication needs. For example, consider:

1. Does your proposed social media account provide a clear benefit for outreach to external stakeholders that is not already met by existing MAJCOM, Wing or headquarters social media efforts?
2. Does the proposed social media account support the commander's mission objectives and help counter damaging misinformation, disinformation and propaganda?
3. Have you developed an effective strategy and communication plan to build a stakeholder audience on social media and to apply existing tools to do so?

4. Has your unit, office or program previously tried engaging stakeholders via social media? If so, was it successful? Why or why not?

All social media sites require active oversight, continuous (usually at least daily) engagements and commitment to actions that sustain them to produce effective results over time. Take these requirements into account when weighing whether to create a new social media presence.

Strategy Development & Content Planning

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

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. For instance, an AF.mil story, live tweets, a blog from the outgoing and/or incoming commanding officer and a social media graphic with a quote can all be generated from prepared remarks requested before the ceremony.

Once released, all Air Force 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 on all your sites. Each platform should be approached with a specific audience in mind. Some content can translate well between platforms. However, you want to tailor the posts to what works best for each.

When content about a single topic is shared on Facebook and Instagram, for example, it's optimized for that platform. A tweet is much shorter (due to Twitter's 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.

After 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. Even though it will save you time, it's not an effective approach. Instead, it indicates you likely don't have the personnel and content to sustain more than one site.

Commanders are responsible for official content posted on their social media. Like a press release or content posted to an Air Force website, information posted to an official social media presence should be approved by a release authority.

These images show how content is tailored for different platforms, namely Instagram and Twitter.

Account Verification

It is recommended that wing-level and above official social media accounts apply for official verification from their hosting social media service. Refer to **Appendix A** for an account verification checklist with instructions on how to submit account verification requests.

Records Management

The use of social media for official business creates federal records that must be captured and managed in compliance with federal records management laws, regulations and policies. Records, regardless of media or security classification, will be created, maintained, used, disposed and preserved to document the transactions of business and mission in wartime and peacetime.

The National Archives and Records Administration outlines how social media records should be captured and managed in compliance with federal records management laws, regulations and policies. See: National Archives and Records Administration Bulletin 2014-02, *Guidance on Managing Social Media Records.*

The Headquarters Air Force Records Manager recently published a records disposition schedule (https://static.e-publishing.af.mil/production/1/saf_cn/publication/afi33-322/afi33-322.pdf) for social media (See section 4.9. Social Media). Units should work with their respective records officers and counsel to ensure compliance.

Branding Guidelines

Each official social media site must include the Air Force or Space Force symbol or approved unit logo or symbol in the profile. The social media site's profile must also include a link (URL) to an official .mil site. Links to .com sites as official pages are prohibited.

Reference AFI 35-114, *Air Force Branding and Trademark Licensing Program and Air & Space Forces Intellectual Property Management*, at https://www.trademark.af.mil/.

Images from the U.S. Air Force and U.S. Space Force Twitter pages.

The images above represent the current banners for the U.S. Air Force and U.S. Space Force Facebook pages, respectively.

Operations Security & Social Media

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 many things public affairs professionals do, use of social media can present OPSEC risks and challenges, but these 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.

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. Carefully consider the level of detail used when posting information anywhere on the internet. Reinforce OPSEC best practices, such as limiting posting information that can be used to distinguish or trace a person's identity to include 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.

Specialized OPSEC training is required for anyone involved in providing Air Force information to the public via official U.S. government websites, including social media sites. Ensure annual OPSEC reviews of organizationally owned, operated or controlled external-facing websites and social media sites are conducted to confirm critical information and indicators are not available to the public. Refer to AFI 10-701, *Operations Security (OPSEC)*.

This checklist can help ensure OPSEC is maintained:

- ⇒ Ensure all personnel involved in the social media process are current on OPSEC training.
- ⇒ Make sure social media content is reviewed by your organization's OPSEC manager and approved prior to posting to social media accounts.
- ⇒ Review your organization's Critical Information and Indicators List prior to posting information.
- ⇒ Make sure your content follows your organization's public affairs and OPSEC guidance.
- ⇒ Monitor your social media streams to make sure fans have not posted OPSEC-violating material.
- ⇒ Help fellow Airmen, Guardians and their families understand the dangers of inadvertent release of critical information.

Find OSD Social Media Education and Training resources at https://dodcio.defense.gov/Social-Media/SMEandT/.

Note: SAF/PAI has determined that OSD's Social Media Education and Training will serve as the primary resource for SM training. As needed, PA shops may develop their own local SM training to augment OSD training but not to replace it.

Security & Password Protection

When online, at work or after-hours, know how to protect yourself and the Air and Space Forces. There are countries, criminals and hackers that are actively going after you as an Airman or Guardian, civilian or family member. Some are trying to get information from you and damage the DAF'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.

Security Best Practices:
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 platforms that track your location. Many use "check-in" functions to broadcast your location, or they 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 – this thwarts efforts by anyone pretending to be you because they won't have access to your alternate/secondary device. Set login notifications on all your accounts so when someone tries to log in from a new location, you get an email and can take action if necessary. Back-up your data. Frequently backup data at home and in the workplace. Many commercial clouds and physical storage devices will encrypt data automatically for extra protection.

Never use a single "shop" administrator account. Multiple administrator accounts are essential for ensuring your team can track team member posting activity.

Strong Password Protocols

- Passwords to all social media channels should be changed regularly (e.g., every quarter).
- Official .mil email accounts should be used when setting up accounts.
- The best password is a string of at least 12-15 random characters containing numbers, upper and lower case letters and symbols.
- Don't use the same password for more than one site or device.
- Don't try remembering all passwords for all platforms and devices. Use a password manager.
- Don't share passwords.
- 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.

A mitigation and remediation plan should be in place and ready to execute in the event of an account security breach, unauthorized access or account compromise. An example of a Social Media Cyber-Vandalism Toolkit (e.g., planning, response, recovery and assessment) is available at https://www.digitalgov.gov/resources/readiness-recovery-response-social-media-cyber-vandalism-toolkit/.

Monitoring/Responding

Engaging with audiences is a key aspect of social media. It is important to check and respond to comments and messages in a timely manner. Monitoring is also referred to as social listening which includes maintaining awareness of current events and social conversations as well as positive and negative feedback. Unmonitored social media accounts are vulnerable to hackers and spam much more than active profiles.

Imposter/Fake Accounts

Impostor accounts violate most social media platforms' terms of service. The best offense is a good defense. Regularly search for impostors and report them to the social media site. Most social media platforms have a reporting system that allows users to report an individual who is pretending to be someone else. Be sure to document the impersonation. Take screenshots of the fake account and copy the URL to reference when you report the account. This helps clarify what account you are referencing and it records the imposter's actions. It is also good to document the accounts in order to track the volume of imposter accounts. Note, it is the decision of the social media platform whether or not to take down a page/profile. The DOD does not own any of the social media platforms.

Sherri Vlastuin, an Army combat medic based at Fort Leonard Wood in Missouri, became popular on Instagram. She wants to use the social media network to inspire young women, but cybercriminals using her photos to engage in "romance scams" have made Vlastuin consider deleting her online presence. (INSTAGRAM)

If a high-level Air Force or Space Force official, such as a general officer, is impersonated, the supporting PAO should contact the platform to submit a removal request. These PAOs should also report imposter accounts linked to MAJCOM and FOA commanders to SAF.PA.Air.Force.Social.Media@us.af.mil.

The best way to combat the issue is to help ensure your audiences and stakeholders know where to find authentic and credible DAF information from .mil and social media sources. Sometimes procedures change for self-reporting accounts, so refer to each platform's help section to find more information about current requirements and options for submitting reports and/or removal requests.

The Department of the Air Force Office of Special Investigation highlights the threats posed by cyber-

criminals who impersonate Department of the Air Force personnel online. AFOSI offers mitigation techniques and address law enforcement's limited ability to investigate these incidents and remove fraudulent accounts. You can also refer to "OSI Cybersecurity: Identifying and Reporting Impostor Accounts."

Bots

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

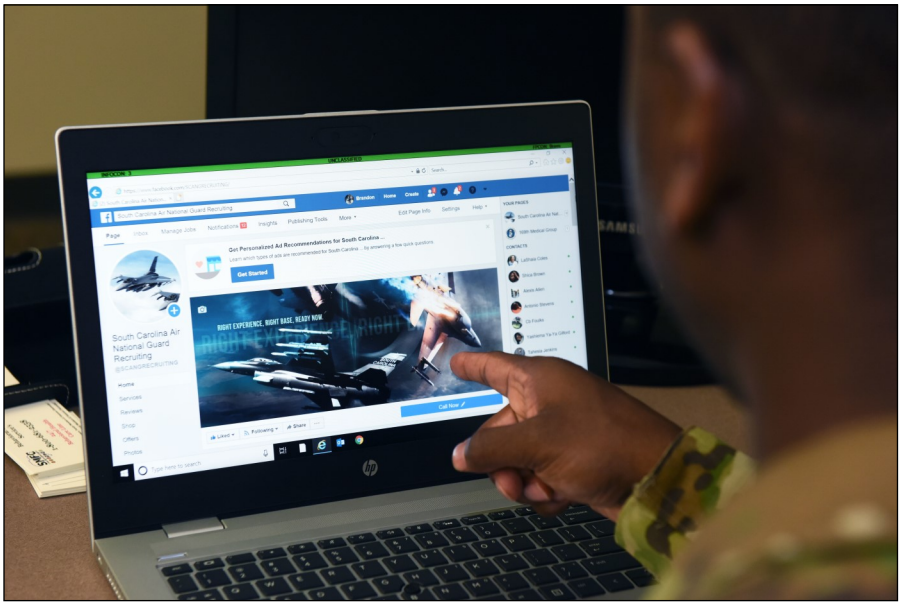


Photo by Senior Airman Mackenzie Bacalzo (DVIDS)

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

Twitter made changes to its application programming interface that would reduce the ability of services that allow links and content to be shared across multiple accounts, which would affect bots. However, bots continue to proliferate on the platform. Be aware that some bots are part of a botnet, or a network of bots that tweet in a coordinated manner. These bots often share the same verbatim tweets and sometimes operate to get specific hashtags trending.

Pay attention to the potential indicators of bots

- Anonymity: The less personal information available on an account, the more likely it belongs to a bot. Look out for usernames that seem to contain too many numbers and generic profile photos. Perform a reverse image search to see if multiple accounts use the same profile photo.
- Activity: Bots frequently engage in suspicious activity. A bot account may have only one tweet with a very high level of engagement or send out a large number of tweets in a short period. Divide the number of tweets by the number of days the account has been active to see how frequently it posts.
- Amplification: Most bots exist to amplify content. On a typical bot timeline, there will be lots of retweets, word-for-word copied-and-pasted headlines and/or shares of news stories without additional comment. There is little original content on a bot account.

You can report bot accounts on Facebook, Twitter, Instagram and YouTube. If you're inundated with com-

ments from bot accounts on a particular post, consider posting one comment with factual information and a source to dispel disinformation.

Crisis Communication

Using social media to communicate with stakeholders during a crisis has proven to be effective due to its speed, reach and direct access. While social media can provide a means for dialogue among the affected and interested stakeholders, traditional sources like press releases and updated unit websites are also essential to distributing command information to key audiences and media.

Post information as it's 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 information that's released and confirmed, post it. You can always post additional information as it's released. If you expect you'll provide updates, say so. Not posting timely updates during a crisis may damage the command's credibility.

Cleared, Credible and Timely Information

To build credibility, you need to establish a presence on social media platforms before a crisis occurs. The best course of action during a crisis is to leverage existing social media accounts. If you have a regularly updated channel of communication before a crisis hits, then your audiences will know where to find information online. Not posting updates quickly during a crisis, or not keeping the community informed, may damage the organization's credibility. Rumors spread faster than ever with social media. Posting accurate information first, and providing subsequent updates, builds credibility and puts your message at the forefront of your audience's mind.

Image from Tyndall Air Force Base's Twitter account.

The best course of action during a crisis is to leverage existing social media accounts. If you have a regularly updated channel of communication before a crisis hits, then your audiences will know where to find information online.

Casualties and Adverse Incidents

Social media distributes official information and 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.

Casualties

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

The media may look at command, Airmen, Guardians, Air Force civilian and family members' social media to get more information. It's important that privacy settings be regularly reviewed to be as restrictive as practical.

It's vitally important that all Airmen, Guardians, DAF civilians, family members and friends know that the identity of a casualty should not be discussed on social media until it's been officially released by the Service.

In accordance with DODI 1300.18, *DOD Personnel Casualty Matters, Policies and Procedures*, no casualty information on deceased military or DAF civilian 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. 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. Don't make your audience search for information. Leverage existing social media presences. For example, if your command is preparing for severe weather, tell your audience where they should go for the latest information.

Image from Offutt Air Force Base's Facebook account.

Correct the Record

Follow what the media reports about your organization and be prepared to respond to misinformation, disinformation, inaccuracy and rumors before they become widespread. If you do not reply with a coordinated response, an inaccurate news story could gain traction. It will be much more difficult to correct additional media reports and the resulting social media conversation if the record isn't corrected as soon as possible.

Images from U.S. Air Force's and U.S. Air Force Academy's Twitter accounts.

Handling Social Media Mistakes

Extensive use of social media may result in occasional mistakes. Follow these steps in the event of a posting error or other mistake:

- Maintain all efforts to remain transparent; edit the post and apologize for the mistake as appropriate, and explain that the material was posted in error and is not an official view. If editing a post isn't an option and a decision is made to delete the post, a screen shot of it should be taken for records management.
- If the mistake was factual, post the factually correct information.

Note: Generally speaking, when Social Media admins insert their personal sense of humor, or positive/negative opinions or commentary, into streams within organizational social media accounts, there is extreme risk that audiences for those streams will construe those posts as reflective of the organization or the Service overall. For this reason, account admins should always avoid the temptation to inject their own humor or opinions into these streams.

Alternatives to Social Media

- Social media is never the right venue for sharing sensitive information. If you have sensitive information you want limited to a specific group, consider one of the Air Force'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 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 the Department of the Air Force, contact the base public affairs officer or your regional 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.

Social Media & Your Command

As an Airman or Guardian, it is vital to understand current and emerging trends and determine the most appropriate approach to incorporate social media into your organization's communication strategy, effectively communicating when, where and how your audience prefers to connect.

Social media can provide a more direct and meaningful way of sharing information about your command while also expanding your reach. This empowers both your internal and external stakeholders to re-share information with their own individual online networks (e.g., friends, family and regional connections).

Additionally, because social media has a truly global reach, it provides public affairs with the means to deter and dissuade adversaries, counter their IW and enhance the trust and support of our allies. Ultimately, social media can be a critical element of public affairs' core competency of global influence.

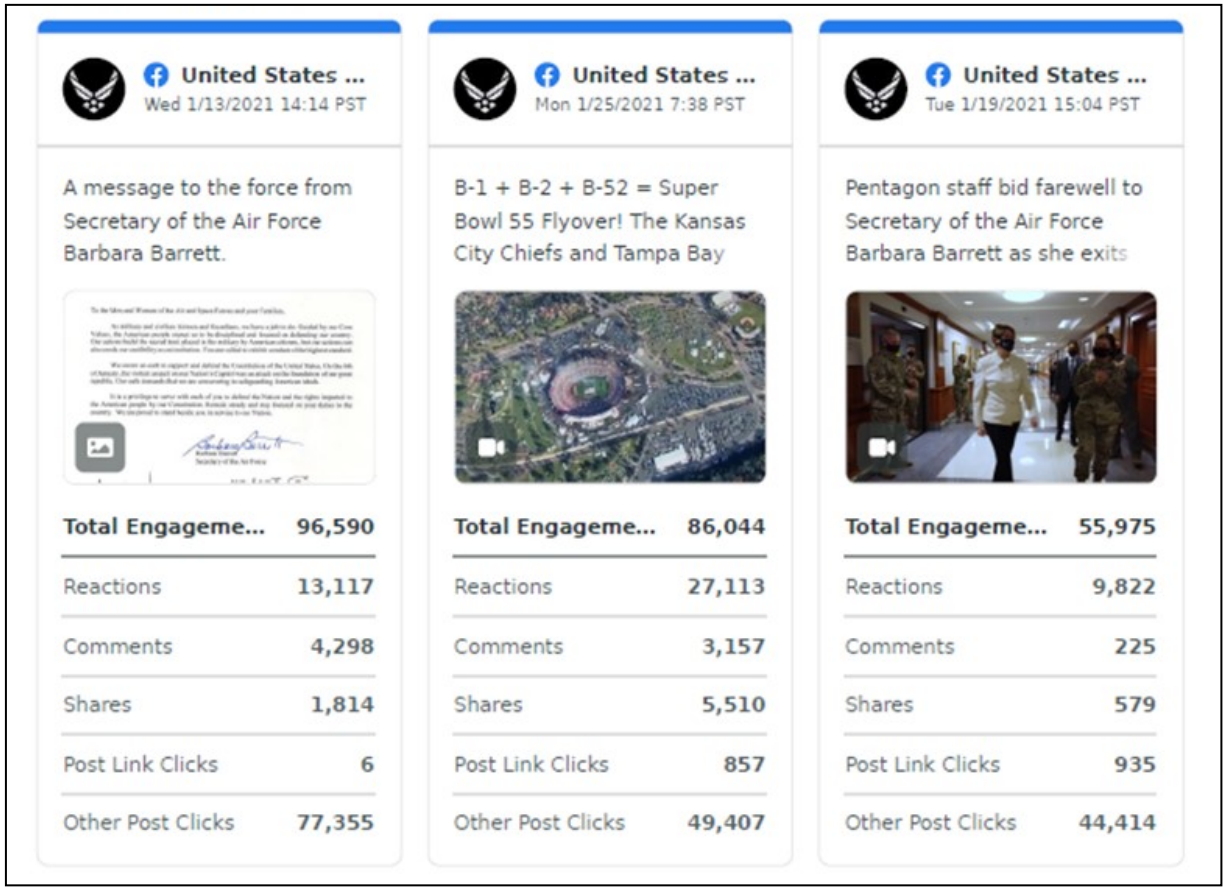
Social Media Management Tools

Social media management tools offer a range of solutions (some free while others are fee-based) that can help you easily organize multiple accounts and share information across several social networks without needing to post anything separately to your accounts directly from the web.

Are you looking for an all-in-one solution to manage your social media presence? Perhaps you need a smarter way to manage multiple profiles and networks? Or maybe you need to improve team collaboration? Social media management solutions can make it easy to:

- Schedule, publish and even share content across social media channels.
- Social listening and engagement with your audience, that includes two-way conversations in real-time.
- Measure the performance of your content.
- Build relationships with new customers, increase your network and reach across earned and owned channels.

There are a number of free and paid social media management tools to consider. Each one has its pros and cons. There's one thing for sure: what suits one PA shop, won't suit another. It's important you choose the right tool for your situation and budget.



This image is an example of how social media management tools can make it easy to measure the performance of posted content.

Whatever your situation, managing social media requires the right strategy and the right tools. When you find the right tool, it will be a game changer for your social strategy.

Note: Mention of any social media platform, available for free or by paid subscription, does not imply or constitute DOD or DAF endorsement. Do research to find the best platform for the management of your command's social media accounts.

Social Media Assessments

To ensure your social media efforts are achieving your aims, you 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 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 your followers, while also communicating command messages.

Assessments are also useful to evaluate one-off events and demonstrate to leadership the importance of social media for communicating DAF messaging.

Tools and techniques for evaluating social media impacts evolve rapidly, but a few general principles apply to any good assessment.

The most important parts of any assessment happen before you post anything. You need an objective, and you need a baseline for comparison.

Objectives describe your desired end state for a particular piece of content, a series of posts, or an account. Good objectives usually make it clear what information should be used to evaluate performance. Common social media objectives include:

- **Virality** – Having content shared to a large number of viewers.

- **Micro-targeting** – Having content shared to or spread by a specific group of people you would like to act on the information. Examples include views and shares of local emergency information by base personnel and families, or mission information that draws positive comments and shares from decision-makers who control policy and funding for that mission.

- **Audience growth** – Increasing the number of people in either the general public or a specific demographic who are following your account or interacting with your content.

- **Interactivity** – Improving how engaging your content is to people who see it regardless of how many people see it. Interaction rates are measured by the number of people who like, share, comment on or click through your post as compared to the larger number of people who viewed the post in their feeds.

Biases in algorithms or the tastes of social media influencers can cap the extent to which official content is likely to go viral or spur audience growth among the general population. In most cases, it generally makes sense to narrow objectives to producing highly interactive content that is effectively micro-targeted and generates audience growth among key groups of people. For example, a social media campaign of videos shot at exercises in Eastern Europe that is designed to reassure partners and deter potential adversaries in that region would focus on users posting from Eastern European countries: positive vs. negative interactions, and the growth in followers from that region during the course of the campaign.

Achieving objectives usually requires a baseline you can compare your performance against. If you do not have a baseline, you can describe what happened with your social media content, but it will be much more difficult to determine whether that outcome was good or bad. Two types of baselines are common:

- **Averages:** How all your social media content performs over a long period of time compared to how well the content linked to your objective performs. For example, if you want to make your Facebook posts promoting diversity and inclusion (D&I) more engaging than most of the rest of your Facebook posts, you could compare the average interaction rate for posts in 2020 with the interaction rate for D&I posts. If your average interaction rate was 4% of viewers and your D&I campaign achieved 8% interaction, you met your objective.

- **Apples to apples comparisons:** Comparing performance involving one event, issue, or organization with performance involving another very similar event, issue, or organization. Posts about your 2020 open house should be compared to posts made during previous open houses. The outcome of a tornado readiness campaign should be compared to other safety campaigns. Your base social media accounts should be compared to other base accounts, preferably bases that share similar missions and therefore tend to attract similar audiences.

Most social media platforms include the basic tools you need to gather data about the accounts you operate. There also are several moderately expensive to very expensive tools and services you can buy that can help you assess social media performance against large chunks of the information environment. Do your research and check with your MAJCOM/PA or SAF/PAX before you make a major investment in social media assessment. PA offices at different levels may have licenses for tools you can use. Many software and services packages require a lot of know-how from users to build elaborate searches, or they do a poor job of measuring the kind of results sought by government organizations vs. corporate clients.

In the end, good assessment demands that you put personal thought and effort into setting objectives, understanding your audience, producing good and timely content, collecting performance data continuously and applying feedback to improve your performance. No automated system can replace the demands that social media success places on your professional time, talents and judgment.

Metrics

Most social media platforms provide integrated analytics to track engagement and reach. However, measuring social media success is much more than counting followers and likes. The Federal Social Media Community of Practice via the beta *U.S. Public Participation Playbook* (https://participation.usa.gov/) provides examples of what PA offices can measure to help determine the value and impact of social media in addressing agency mission and program goals. Suggested metrics include call-to-action engagement rates, hashtag use, comment sentiment/amounts, post mentions/shares, length/number of video views, website directs from social media platforms, URL click rates, etc. Note: There is no mandate/policy for PAs to develop or report metrics. It is a commander's decision to make whether it is desired at the local level.

Key Performance Indicators (KPIs)

What variables will you look at to indicate the success of your content? Examples:

- views/impressions
- shares
- X number of engagements per quarter
- X increase in followers
- X increase in reach per quarter
- X number of clicks on linked URL

Online Advertising

With very few exceptions, Department of the Air Force accounts may not pay to boost Facebook posts, promote tweets or take similar action on content. DAF 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." Failure to follow this rule may be a violation of 5 C.F.R. §2635.702 and DOD 5500.07-R, Joint Ethics Regulation §3-209. Consult your command's judge advocate general or contracting officer for exceptions and addi-

Courtesy image (DVIDS)

Podcasts

The evolution of podcasting as a format has transformed it into a powerful tool. Podcasts now provide a useful form of owned content that many PA professionals use as part of an integrated communication strategy. More specifically, an organization can closely control how its podcasts are recorded, edited and distributed so they reach the right audiences with relevant content.

The images here are examples of graphics used to promote podcasts. (AF.mil)

A successful podcast strategy can be built upon close attention to many technical details, as well as adept management of a show's subject matter and guests. Some reliable podcast best practices include:

- **Using high-quality equipment.** A suitable mic, mic stand, mixer, headphones and editing software is preferable to recording with a smartphone or tablet, as the quality will come through and make the show seem more professional.
- **Lining up the right guests.** Interviews and guest conversations are great ways to diversify a podcast's content and increase its visibility.
- **Marketing the show across social media.** Podcasts should be part of an integrated social media strategy. Accordingly, it makes sense to promote them on channels such as Instagram and Twitter to raise awareness and grow their audiences.
- **Creating a great introduction.** A podcast is similar to a radio show. As such, it should have an interesting intro that piques the audience's interest and creates a distinctive impression of the show.
- **Choose the right podcast format for your show.** Your podcast format explains how many voices are on your show, as well as their purpose. Sometimes there's only one voice carrying the entire episodes. Other times, there's a host who brings in a guest or small audio snippets from many voices. Or perhaps it's somewhere in between. While it's good to have a "regular" format so your listeners know what to expect, you don't have to stick to it every time. Mix it up a little from time to time. Experiment and ask your listeners what they think. That's the driver for change, for innovation in your show, and that's what keeps people interested, alongside stimulating, relevant content, of course.

Example: See **Appendix F** for Air Force Television's podcast production workflow checklist, an outline of the Air Force podcast creation process from setup to distribution.

Live Streaming

In our current environment there's an almost endless amount of options for "going live" between Zoom, DVIDS, YouTube and within social media platforms. But the biggest commonality between them all is that they require solid and reliable connectivity. A best practice: anyone planning to host a live "town hall"-like event should test connectivity 24 hours out and again as soon as an hour out to ensure the stream works and people are able to see it. Otherwise, if viewers can't see/hear your livestream, they will get frustrated and leave.

Taking Murphy's Law into account, another best practice is to have standby posts on hand in the case the livestream completely fails to function properly. Have something drafted that will divert traffic to either an alternative place to view the livestream or to standby through technical difficulties.

It's a good idea to have a plan before you dive in. Field questions prior to the event in order to prepare the person hosting. More often than not, the questions you field prior to the livestream are a good pulse on questions you'd receive from a live audience.

Photo by Peter Borys (DVIDS)

914th ARW commander conducts town hall live stream

Col. Mark Larson (far left), 914th Air Refueling Wing commander, and Maj. Erlin Marte (far right), 914th Aeromedical Staging Squadron flight surgeon and public health emergency officer, answer questions via live internet streaming while 2nd Lt. Lucas Morrow, 914th ARW public affairs officer, facilitates the event at the Niagara Falls Air Reserve Station, N.Y., April 9, 2020. The two answered questions concerning a range of topics pertaining to the current COVID-19 crisis from members of the unit and their families.

For detailed information about livestreaming, see:

- How to live stream to Facebook: https://www.facebook.com/help/publisher/626637251511853
- How to live stream on YouTube: https://support.google.com/youtube/answer/2474026?hl=en
- How to go live on Instagram: https://help.instagram.com/292478487812558

For information about video telecom, see:

- How to use Google Hangouts: https://support.google.com/hangouts/answer/3110347?co=GENIE.Platform%3DDesktop&hl=en-GB

Guidelines for Airmen, Guardians, DAF Civilians & Families

Social Media & Leaders

Commanders should base and tailor their decisions about how to use various social media on specific, intended outcomes they expect social media to contribute as they pursue their communication missions and objectives. This tailored approach could involve an official unit presence on a social media platform, or an official presence by the commander exclusively, or both.

When using social media in an official capacity, it's important to be honest about who is posting information on behalf of senior leaders. It's a best practice to separate official accounts from personal accounts. Of course, leaders can have personal social media accounts to communicate with family and friends, but these accounts should be distinct from the official account which distributes information on behalf of the U.S. Air Force. AFI 1-1, *Air Force Standards* outlines how leaders can use social networking sites.

Leaders are reminded to maintain appropriate standards in their communication and conduct with all personnel, peers, superiors and subordinates (to include civilian superiors and subordinates). If personal social media accounts are publicly viewable and show an Air Force affiliation, public viewers of photos, videos, posts and comments can reasonably perceive that this content portrays the values and beliefs of the Air Force as a whole.

Social Media & DAF Members

AFI 1-1, *Air Force Standards*, chapter 2 includes information on how Airmen and Guardians should conduct themselves on social networking sites. Here are a few things to remember when communicating online via social media as an Airman or Guardians: DAF personnel are personally responsible for what they say and post on social networking services and any other medium. Airmen and Guardians must consider how a post can be interpreted by the public. They must be cautious about crossing the line between funny and distasteful. When in doubt about whether to post something, Airmen and Guardians should err on the side of caution. If the post in question concerns the Air Force, discuss the proposed post with a supervisor or your local public affairs office.

Best Practices for Social Media Use:

1. No classified information. **Do not** post classified, sensitive or For Official Use Only information (for example, troop movement, force size, weapons details, etc.). If in doubt, talk to your supervisor or security manager.
2. Stay in your lane. Discussion of issues related to your career field or personal experiences are acceptable and encouraged, but you shouldn't discuss areas of expertise where you have no firsthand, direct experience or knowledge.
3. Obey applicable laws. Always keep federal law, DOD directives and instructions, Air Force instructions and the Uniform Code of Military Justice in mind when using social media in official and unofficial capacities. As an Airman or Guardian, you are on duty 24 hours a day, 365 days a year.
4. Differentiate between opinion and official information. Say what you think…just make sure you state that this is your opinion and not that of the organization.
5. Use your best judgment. Written statements may have serious consequences. Once you post

truly gone. Ultimately, you bear sole responsibility for what you post.

6. Replace error with fact. When you see misrepresentations made about the Air Force in social media, you may certainly identify and correct the error. Always do so with respect and with the facts. When you speak to someone who has an adversarial position, make sure what you say is factual and respectful. Don't argue, just correct the record.
7. Any time you engage in social media, you're representing the DAF. Don't do anything that discredits you or our service.
8. Maintain privacy settings on your social media accounts, change your passwords regularly and don't give out personally identifiable information. Be cautious about the personal details you share on the internet.
9. Don't post defamatory, libelous, vulgar, obscene, abusive, profane, threatening, racially or ethnically hateful or otherwise offensive or illegal information or material.
10. Don't post information that would infringe upon the proprietary, privacy or personal rights of others.
11. Use caution when geotagging. Be careful when allowing access to geographical identification data to photos, videos, websites and text messages through location-based applications. Access could potentially create personal and operational security risks. Disable geotagging at sensitive or deployed locations.
12. Don't post any information or other material protected by copyright without the permission of the copyright owner.
13. Don't use words, logos or other marks that would infringe upon the trademark, service mark, certification mark or other intellectual property rights of the owners of such marks without owner permission. The Air Force and Space Force logos visually represent the services' brand identity. To use the Air Force symbol on a social media platform, everyone must follow display guidelines found at http://www.trademark.af.mil.
14. Don't use the Air Force name to endorse or promote products, political positions or religious ideologies.
15. Don't manipulate identifiers in your post in an attempt to disguise, impersonate or otherwise misrepresent your identity or affiliation with any other person or entity.
16. Don't promote yourself for personal or financial gain. Don't use your Air Force affiliation, official title, or position to promote, endorse or benefit any profit-making group or agency, or non-profit groups based solely on religious or political affiliations, IAW DODD 5500.07, and AFI 1-1, *Air Force Standards*. This includes appearing in, or preparing statements for inclusion in, advertisements designed for use by electronic or print media.
17. Become familiar with each social media platform's terms of service and follow them. For example, having two personal profiles on Facebook violates their terms of service.

Social Media & DAF Families

Family members are integral to the success of the Air and Space Forces. Without their support, Airmen and Guardians couldn't accomplish the great work they do every day. Stories Air Force family members share on social media can help maintain the morale of Airmen and Guardians and educate the public about the Air and Space Forces.

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

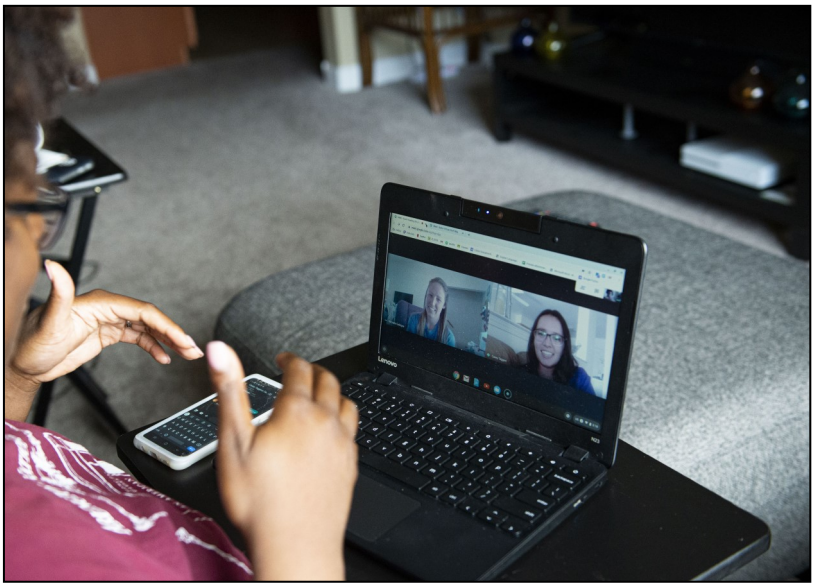


Photo by Staff Sgt. Julian Kemper (DVIDS)

- Social content shared by Airmen, Guardians and their families is a major target for those looking to gain access to sensitive information in order to impersonate, blackmail or intimidate. While there is a definite benefit to using social media, be wary of the details you provide.
- Don't post the exact whereabouts and activities of deployed Airmen and Guardians.
- Be general about the dates and locations concerning a member's trip arrival and departure.
- Don't make your vacation dates public on social networks. Criminals may track your activities and know exactly when to break into your home.
- Don't publicly post exactly how long your Airman or Guardian will be gone on a trip or deployment.
- Be careful about publicly posting children's photos, names, schools, ages and schedules.
- Consider the image you portray on social media. Think before you share information that could jeopardize you and your Airman's or Guardian's career or reputation.
- Let children know they should seek help for cyber-bullying.

Family members are encouraged to use social media to engage in support networks, such as spouse's clubs, event committees, childcare groups or local civic activities. These groups are not considered official Air Force social media presences, and you don't need permission to form a group of your own. Limiting the membership and visibility of the group can help protect the information exchanged. Even if the membership and visibility is limited, sensitive information should never be discussed online.

Family members may also want to follow the main Air Force social media accounts (listed at the end of this document), or local base's accounts for the latest information on the work your Airman does, and to share social media content and experiences with followers and friends.

Online Conduct

Improper or inappropriate online behavior by Airmen, Guardians and DAF civilians, should NOT be tolerated and should be reported if experienced or observed. When it comes to command leadership, your

conduct online should be considered no different from your conduct offline.

If evidence of a violation of command policy, Uniform Code of Military Justice or civil law by an Airman, Guardian or DAF civilian in your command comes to your attention from social media, you should act on it immediately. Refer the incident to the individual's leadership and their supporting LE/OSI agency for investigation and action as appropriate.

Airmen and Guardians using social media are subject to the UCMJ and Department of the Air Force regulations at all times, even when off duty. Commenting, posting or linking to material that violates the UCMJ or Department of the Air Force regulations may result in administrative or disciplinary action, to include administrative separation, and may subject DAF civilians to appropriate disciplinary action. Punitive action may include 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. Refer to AFI 1-1, *Air Force Standards*, Chapter 2 for information on how Airmen and Guardians should conduct themselves in the digital environment.

Lastly, if you're expressing a personal opinion of any kind, it's your responsibility to make clear you're not speaking for the Air Force and that the stance is your own and not representative of the views of the Air Force.

Political Activity

Airmen & Guardians

The primary guidance concerning political activity for Airmen and Guardians is found in AFI 51-508, *Political Activities, Free Speech and Freedom of Assembly of Air Force Personnel*. Per longstanding DOD policy, active-duty personnel may not engage in partisan political activities and Airmen and Guardians should avoid the inference that their political activities imply or appear to imply DOD sponsorship, approval or endorsement of a political candidate, campaign or cause.

Airmen and Guardians may not campaign for a partisan candidate, engage in partisan fundraising activities, serve as an officer of a partisan club or speak before a partisan gathering. Active-duty members may, however, express their personal opinions on political candidates and issues, make monetary contributions to a political campaign or organization and attend political events, in their personal capacity as a spectator when not in uniform.

DAF Civilians

The political activity of DAF civilians is regulated by a number of sources: the Hatch Act (5 USC 7321 – 7326), regulations (5 CFR 733 and 5 CFR 734), as well as DOD policy. For purposes of the Hatch Act, political activity is defined as "an activity directed toward the success or failure of a political party, candidate for partisan political office or partisan political group."

DAF employees may not engage in political activity while on-duty or in a federal building. Specifically, an employee may not send or forward political emails, post political messages to social media, such as a

Facebook account or political "tweeting" while in a federal building (including when off-duty), even if the employee is using their personal smartphone, tablet or computer. Employees may not use government equipment to engage in political activities. See Hatch Act Guidance on Social Media, US Office of Special Counsel, February 2018.

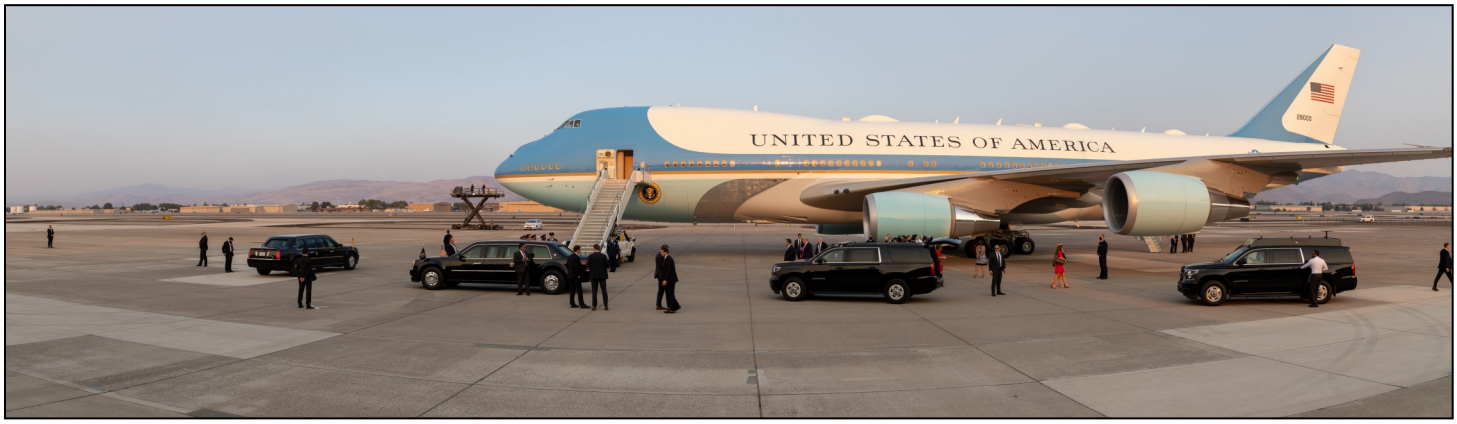


Photo by Staff Sgt. Matthew Greiner (DVIDS)

Politics & Social Media

DAF civilians may generally express their personal views on public issues or political candidates via personal accounts on social media platforms, such as Facebook, Twitter or personal blogs, in the same way they could write a letter to the editor of a newspaper. If, when expressing a personal opinion, personnel are identified by a social media site as a DOD employee, the posting must clearly and prominently state that the views expressed are those of the individual only and not of the Department of Defense.

While Airmen, Guardians and DAF civilians may "follow," "friend" or "like" a political party or candidate running for partisan office, but they may not post links to "share" or "re-tweet" comments or tweets from the Facebook page or Twitter account of a political party or candidate running for partisan office. Such activity is deemed to constitute participation in political activities.

Social media guidance for military members [FAQs Social Media and Political Activities - Guidance for Members of the Armed Forces (June 24, 2014)] and DAF civilians [Social Media and the Hatch Act and Social Media Quick Guide] offers advice on how to avoid violating the rules.

Resources:
For more information on the Hatch Act or DOD Directive 1344.10, *Political Activities by Members of the Armed Forces*, personnel should contact their local legal or Staff Judge Advocate office.

General guidance on the Hatch Act can be found at the U.S. Office of Special Counsel website, www.osc.gov.

Endorsements

Air Force 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 Airman or Guardian may solicit gifts or prizes for command events in any capacity — on duty, off

duty or in a personal capacity. Reference the Air Force Ethics Office (SAF/GCA), which provides ethics leadership to all Air Force personnel through training, education and case-specific guidance, offering legal advice to ensure public confidence in the integrity of government officials.

Reporting Incidents

Anyone who experiences or witnesses incidents of improper online behavior should promptly report it as soon as possible to the Air Force Office of Special Investigations. Consult your base phone book or call your base operator for the telephone number of your base's AFOSI unit.

If you do not have a base telephone book and don't know the number to the base operator, call toll free 1-877-246-1453 for the phone number of the AFOSI unit nearest you.

More information about reporting social media incidents of concern is located in **Appendix D**.

Photo by Louis Briscese (DVIDS)

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 users and their systems to security weaknesses. Information you share on the internet can provide terrorists, spies and criminals information they may use 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 any time. 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).

Cyberbullying

While social media sites allow people to connect with loved ones and friends, they also provide new opportunities for bullying and harassment. Families of Airmen and Guardians should engage in respectful conduct on social media and report improper online behavior when appropriate.

According to a study conducted in 2018 by Pew Research Center, ("A Majority of Teens Have Experienced Some Form of Cyberbullying," September 27, 2018, https://www.pewresearch.org/internet/2018/09/27/a-majority-of-teens-have-experienced-some-form-of-cyberbullying/), 59 percent

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 percent). About a third (32 percent) of teens say that someone has spread false rumors about them online, while 21 percent have had someone other than a parent constantly ask where they are, who they're with or what they're doing, and 16 percent have been the target of physical threats online.

If you experience bullying or harassment on social media, you can report a user, message or post in-platform. Facebook, Twitter 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.

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

DODI 1020.03, *Harassment Prevention and Response in the Armed Forces*, establishes a comprehensive DOD-wide military harassment prevention and response program and updates military harassment prevention and response policies and programs for service members. It states bullying, including by means of social media, "is prohibited in all circumstances and environments, including off-duty or 'unofficial' unit functions and settings."

Any member of the Air Force community experiencing or witnessing incidents of improper online behavior by an Air Force community member should report the activity to their chain of command. Refer to **Appendix E** for more information regarding cyberbullying.

Contacts & Acknowledgements

Contacts

For comments or to provide content updates to this guide, contact:
Angelita Colón-Francia, Public Web and Command Information Policy Lead
Secretary of the Air Force Public Affairs – Command Information Division
angelita.colon-francia.1@us.af.mil

To reach the Air Force Digital Media Team or Space Force Digital Media Team, email SAF.PA.Air.Force.Social.Media@us.af.mil.

Acknowledgements

Thanks to DAF subject matter experts who have contributed to the update of this guide. Special acknowledgement is extended to Defense Media Activity, Air Force Public Affairs Agency and the U.S. Navy social media team.

Appendix A

Social Media Account Verification Request Checklist

Senior leader and/or Wing-level and above accounts seeking verification via platforms offering this option should have an account transition "sunset plan" as part of the social media plan or communications plan.

Request Verification for Official Wing-Level and Above or Senior Leader Accounts (Verification adds another layer of credibility to social media communications channels; however, verified status is not guaranteed. Platforms frequently change criteria for verification. Each social media platform has a different verification process. Please visit each to apply for official verification status for your command's social media accounts.

⇒ Account has a dedicated Public Affairs Officer or Social Media Manager

Per DOD guidance, it is recommended that only accounts with a dedicated Public Affairs Office and a written strategy plan should apply for official verification from specific social media sites.

⇒ Account communication/social media plan AND "sunset" plan

Per DOD guidance, it is recommended that social media accounts have a written strategy plan and dedicated Public Affairs Office. The plan should also include instructions for transitioning or dissolving "sunset" senior leader and/or other (e.g., Wing-level and above) official social media accounts.

⇒ Twitter

Twitter will verify an account of public interest as authentic. More information is available at https://support.twitter.com/.

⇒ Facebook

Submit requests to SAF.PA.Air.Force.Social.Media@us.af.mil. Facebook provides verification for some pages and profiles to confirm the accounts are authentic. Facebook will add an identifier on a page or profile it has authenticated as belonging to a public figure, media company or brand.

Appendix B

Social Media Registry Checklist

All official social media accounts must be submitted to the Air Force Social Media registry at http://www.af.mil/AFSites/SiteRegistration.aspx.

Register All Official Air Force Social Media Accounts

Register all official Air Force social media sites (web presences). All submissions, if approved, will be added to the DAF social media registry.

- ☐ **Account approved by public affairs office (or commander, if applicable)**
  Accounts/presences (including names and logos) must be reviewed and approved by your public affairs office prior to submitting to the AF social media registry.
- ☐ **Account included in a communication plan or social media plan**
  Per DOD guidance, it is recommended that social media accounts have a written strategy plan and dedicated Public Affairs Office.
- ☐ **Account set-up as appropriate type/category**
  For example, official Air Force Facebook organization accounts should be created as a "Government Organization" page (unit) or "public figure" page (individual person) not as a "business" page.
- ☐ **Account links to an official AF.mil website or senior leader biography**
  A URL linking to an official Air Force website should be prominently displayed on the account profile or in other appropriate sections of the social media account. Accounts can include/list other official social media platforms but those sites do not replace the AF.mil reference.
- ☐ **Account comment policy AND rules of engagement**
  Include comment policy and posting guidelines or a URL link to another official AF site that explains what is permissible.
- ☐ **Account is active and has content not older than 30 days**
  Social media account manager ensure posts occur at least monthly on each platform. If an account has not been used for 30 days or more, you need to re-evaluate your communication plan and determine if the social media account is still needed to achieve communications goals and objectives.
- ☐ **Account owner(s)/manager(s) OPSEC training and compliance**
  In addition to completing OPSEC training, the account owners and managers must ensure the social media presence adheres to operations security guidelines. AFI 10-701 requires the completion of two OPSEC courses for Public Affairs (see Table 4.7). Completion is mandatory for all PA military officer and enlisted AFSCs and PA civilian occupational series. Both courses are one-time training requirements (para 4.4):
  a. OPSE 1301, OPSEC Fundamentals is a 60-minute course available on ADLS (https://golearn.adls.af.mil/login.aspx).
  b. J3O P-US1322, AF Identity Management is a 30-minute course on Joint Knowledge Online (https://jko.jten.mil/).

  Upon completion of the Air Force Identity Management Course, people should provide their unit training manager a copy of their completion certificate to upload into their training records. These courses supersede the requirements of the previous version of AFI 10-701 (June 2011), which required OPSE 1500 (OPSEC and Public Release Decisions) and OPSE 3500, OPSEC and Internet-Based Capabilities.
- ☐ **Site is unlocked (e.g., not a private group or platform) and is publicly accessible via the internet**
  Official social media accounts/presences used for external communication and public affairs purposes must be publicly accessible.
- ☐ **Branding (official names and logos) is uniform across all social media platforms**
  Official branding should be in accordance with DAF and DOD regulations.

Appendix C

Tips to Stay Safe Online

1. Post appropriate content.

- You are personally responsible for your actions.
- Ensure DAF content you post is accurate and appropriate.
- Remember: you lose control over content once it's posted.
- Always use your best judgment and keep in mind how the content of posts will reflect upon yourself, your command, and the DAF – now and in the future!

2. Don't break the law.

- Adhere to federal law, as well as Department of Defense and Department of the Air Force regulations and policies.
- Don't use any words, logos or other marks in your posts if it will infringe upon the trademark, service mark, certification mark or other intellectual property rights of the owners.
- If you violate federal law, regulations or policies, you are subject to disciplinary action under the Uniform Code of Military Justice.

3. Understand the guidelines when making unofficial posts about the DAF.

- If appropriate, identify yourself as an Airman or your affiliation with the Air Force, to include your rank, military occupational specialty or occupational series, and status (active, reserve, civilian, contractor).
- If you decide not to identify your affiliation with the Air Force, you should not disguise, impersonate or otherwise misrepresent your identity.
- You can use Department of the Air Force symbols in unofficial posts so long as the symbols are used in a manner that does not bring discredit upon the services, does not result in personal financial gain, or does not give the impression of official or implied endorsement.

4. If you wouldn't say it to your grandma, don't post it.

Don't say/post anything that could be perceived as:

- Defamatory
- Libelous
- Obscene
- Abusive
- Threatening
- Racially or ethnically hateful
- Otherwise offensive or illegal

5. Avoid spillage!

Do not post any information that is:

- Classified (Confidential, Secret, Top Secret)
- Controlled Unclassified Information
- Sensitive but Unclassified (SBU), For Official Use Only, Law Enforcement Sensitive, Sensitive Homeland Security Information, Security Sensitive Information, Critical Infrastructure Information, etc.).
- In violation of operations security (OPSEC), such as tactics, troop movements, force size, weapon system details, and so on.
- When in doubt, contact your unit operations officer, security manager, intelligence officer, foreign disclosure officer or public affairs officer for guidance.

6. Guard your personal information.

- Do not provide sensitive, family-related information within your profile.
- Keep your plans, schedules and location information to yourself.
- Protect your coworkers, friends and family members. Don't post information that would infringe upon their privacy, proprietary, or personal rights. This means: don't post their personal contact information such as email address, home address, phone numbers, Social Security number or physical location.
- Tell friends to be careful when posting photos and information about you and your family. Talk to family and friends about operations security and what can and cannot be posted.
- Videos can go viral quickly; make sure they don't give away sensitive information. When using social media, avoid mentioning rank, unit locations, deployment dates, names, equipment specifications and capabilities.
- Geotagging is a feature that reveals your location to other people within your network. Consider turning off the GPS function of your smartphone. If you're involved in an official exercise, operation, or deployment – turn off your mobile device's GPS functions.

Don't share your:

- Social Security number
- Home address
- Birthday
- Birth place
- Driver's license number
- Other personally identifying information

- By piecing together information provided on different websites or from different responses, criminals and adversaries can use the information to, among other things, steal your passwords and identity, impersonate you, stalk you, harm you, harm your family and harm your fellow Airmen and Guardians.
- Check all photos you intend to post for indicators in the background or reflective surfaces that may expose unwanted details.
- Double check that you want the information you are about to post to be forever available to anyone at anytime.

Tips (Continued)

7. Don't share information that is not approved for public release.

• Not memos, not e-mails, not meeting notes, not message traffic, not white papers, not public affairs guidance, not pre-decisional materials, not investigatory information, not proprietary information… JUST DON'T DO IT!

8. Talk about what you know best.

• Only discuss Air Force or Space Force issues related to your professional expertise, personal experiences or personal knowledge.

9. Correct misinformation politely.

• Professionally and respectfully correct errors and misrepresentations made by others about the DAF.
• Not sure if you have accurate information to correct an error? Refer to your chain of command or public affairs office for guidance.

10. Don't get political.

• If you do want to provide your political opinion, do so within Department of Defense guidelines:
• You can express your political views on public issues or political candidates online, but not as part of an organized communication campaign.
• If your communication identifies you as a member of the DOD or DAF you should clearly state the opinions are yours.
• You cannot solicit votes for or against a party, candidate or cause.
• You cannot participate in any interview or discussion as an advocate for or against a party, candidate or cause.
• Commissioned officers must avoid contemptuous words against the president, vice president, secretary of defense, deputy secretary of defense, secretary of DAF or governor and legislature of any state in which he or she is located, or performing duty in. This is federal law.
• Don't express or imply Air Force endorsement of any opinions, products or causes.

11. Look out for bad guys.

• Do not click links or open attachments unless the source can be trusted.
• Cyber criminals pretend to be people they are not in order to deceive you into performing actions that launch cyber-attacks, download viruses and install malware and spyware onto government or personal computers.
• Look for "HTTPS" on the web site address and the "lock" icon on the web page that indicate active security before logging in or entering sensitive data (especially when using Wi-Fi hotspots).

12. Don't fire and forget – review all your account and privacy settings.

• "Friends" and "followers" are considered relationships that can affect your security clearance, so make sure you only make connections with people you know well.
• Sort "friends" into groups and networks, and set access permissions accordingly. Add "untrusted" people to the group with the lowest permissions and accesses.
• Verify, through other channels, that a "friend" request was actually from your friend.
• Beware of apps or plug-ins, which are often written by unknown third parties who might use them to access your data and friends.
• Applications may share your personal information with other users on Facebook AND external to Facebook. Check the settings of EACH application you use before "allowing access."
• Make sure only your family and friends (people you know WELL) can see your photos, full name, and other information.
• Assume that all the information you share will be made public (meaning, someone can find it on Google).
• Don't accept default account privacy settings. Carefully look for and set all your privacy and security options – in all your online accounts (not just Facebook).

13. Use strong passwords.

• Whenever possible, use at least 14 characters or more.
• The greater the variety of characters in your password, the better.
• Use the entire keyboard, not just the letters and characters you use or see most often.
• Have a different password for every login.
• When creating a password avoid: Dictionary words in any language, words spelled backwards, common misspellings and abbreviations, sequences or repeated characters and personal information.

14. Look out for intruders.

• Notice any changes to your account that you didn't make? Change your password immediately.
• Think about how someone may have received access to your site and make appropriate changes to avoid that in the future.
• Check your accounts daily for possible use or changes by unauthorized users.

15. Use anti-virus and anti-spyware.

• Use anti-virus and anti-spyware software on your personal computer and keep them up to date.

Appendix D

Reporting Social Media Comments of Concern

1. **Comments on Social Media that Require Attention.** Rarely, but occasionally, public comments are of concern to other offices in DAF. To expedite processing, the public affairs office should discuss with local installation offices what they expect and which people or organizational emails should be used to report social media comments of concern.

2. **Threats of Harm.** Any threat of harm should be taken seriously. Make an image of the threat on screen, then forward it to the local command post, security police and Judge Advocate Office. Call immediately to ensure someone in each of those offices has seen the post. Hide the post on the social media platform. Do not permit a post threatening harm to go live on the social media platform, as this kind of public attention may be what the individual is seeking.

3. **Suicidal Ideas.** Any indication of intent to do self-harm should be taken seriously. Image the screen with the comment, and forward it to the unit commander, local first sergeant and/or senior enlisted leader, command post, security police and Judge Advocate Office. Call immediately to ensure someone in each of those offices has seen the post. If you can identify the individual and find them in the global address listing, send the screenshot to the first sergeant or appropriate leadership in the unit. Hide the post on the social media platform.

4. **Allegations of Wrongdoing**. Any allegations of wrong doing by DAF employees should be taken seriously. Image the allegation on screen, and forward to the local Office of Special Investigations or Security Forces. Request an email return receipt requested. Within three days, confirm the office has the information to take for action. Do NOT hide the post on the social media platform. Allegations of wrong doing fall under freedom of speech protections and should not be hidden unless they are filled with profane language or include Privacy Act protected information or another reason to limit distribution.

5. **Posts Including Sexually Explicit Imagery or Videos.** With the publication of the National Defense Authorization Act of 2018, the UCMJ was updated with article 117a to criminalize unauthorized distribution of imagery. Image the post on screen, but do NOT forward the screen shot in an email to the local Judge Advocate Office unless asked to do so. Send a text-only email to the Judge Advocate Office advising them of the nature of the post and they will come to the public affairs office to examine the evidence. Request an email return receipt requested. Within three days, confirm the office has the information to take for action. Hide the post from public view.

6. **Crime Evidence Chain of Custody.** Keep in mind that any of the above posts could become evidence in an investigation. Treat these screen shots the same way forensic photographs are handled. Work with the local law enforcement and legal offices to ensure proper chain of custody for action.

Appendix E

Cyberbullying

While no one-size-fits-all plan to address bullying exists, Military OneSource recommends adults create a strategy for monitoring a child to determine what triggers bullying behavior. It also recommends working with schools to set up programs to address bullying and provide examples of positive behavior and problem-solving techniques. Additional resources to help parents, educators, and children prevent or address bullying – including cyberbullying – are available from Military OneSource and Stop Bullying.

Report Cyberbullying

When cyberbullying happens, it is important to document and report the behavior so it can be addressed. If evidence of a violation of command policy, Uniform Code of Military Justice or civil law by an Airman, Guardian or DAF civilian in your command comes to your attention from social media, you should refer the incident to the individual's leadership and their supporting LE/OSI agency for investigation and action as appropriate.

Steps to Take Immediately

- Don't respond to and don't forward cyberbullying messages.
- Keep evidence of cyberbullying. Record the dates, times and descriptions of instances when cyberbullying has occurred. Save and print screenshots, emails and text messages. Use this evidence to report cyberbullying to web and cell phone service providers.
- Block the person who is cyberbullying.

Report Cyberbullying to Online Service Providers

Cyberbullying often violates the terms of service established by social media sites and internet service providers.

- Review their terms and conditions or rights and responsibilities sections. These describe content that is or is not appropriate.
- Visit social media safety centers to learn how to block users and change settings to control who can contact you.
- Report cyberbullying to the social media site so they can take action against users abusing the terms of service.

Appendix F

THE AIR FORCE PODCAST

PRODUCTION WORKFLOW CHECKLIST

AIR FORCE TELEVISION

1 SETUP

Podcast Assigned by Team Leads or Superintendents
- Initial meeting with team
- Gather any additional information needed to begin project
- Ensure project has been entered/updated in WAR and SMARTS

Meet/talk to requesting customer
- Discuss communication objectives, messaging & audience
- Identify possible interviewees, SMEs and other valuable resources
- Discuss initial dates for recording, drafts, final master delivery & release date

Determine podcast format
1. One-on-one interview
2. Panel (guest interview or discussion)
3. Solo commentary
4. Nonfiction narrative storytelling
5. Hybrid
6. Repurposed content

2 PRE-PRODUCTION

Research & Planning
- Gather articles, reports, bios, and media on subject/topic
- Prepare interview questions or determine flow of conversation
- Write script/outline if using multiple sources

Location
- Studio is best, gives the most control of environment
- On-location scouting/site survey if needed

Scheduling
- Book date, time and location of recording
- Build crew based on requirements
- Send calendar invites to principals, crew and advisors

Equipment

Determine best gear and equipment to use to include:
- Microphones
- Audio Recorders
- Cameras, Tripods and Lighting (if neccessary)

3 PRODUCTION

Have outline, script or questions before you start audio production

Keep in constant contact with and regularly update crew
- Determine times for setup, crew calls and show times
- Determine attire (ABUs, Blues or Media Training clothes)
- Articulate roles and responsibilites

Pull/test gear (24 hrs) prior to recording
- Fill out equipment list and property pass if off-site

Brief talent and review best practices

Conduct sound test to ensure best mic and talent placement

Conduct a hot wash & review footage after recording

Practice good media managment throughout production
- Label all footage by location, date, and subject
- Backup footage on Blueserver

4 POST-PRODUCTION

Ensure you have all the recorded media you need to start editing

Clean up audio, adjust levels and remove any unwanted noise

Get plenty of feedback before presenting 1st draft

Conduct internal review with Team Lead/Superintendent

Delivering draft to POC/Customer
- Export h.264 MP4 file (with graphic) and MP3 file
- Upload to AFBlueTube and leave unlisted
- Add to PA drive under AFTV Proofs folder

Repeat draft process until final approval

Finalize and master podcast for distro and archive
- Remove/archive drafts and previous versions

Send final podcast files to customer

5 PROMOTION

Create graphics (.jpg) for thumbnail and promotion
1. 1920x1080 graphic for video and social media
2. 1000x1000 graphic for video and social media

Create video previews to promote podcast episode
- 1-3 previews highlighting different moments
- 30-90 seconds in length
- Export h.264 MP4 files in 1080p and square (1000x1000)

Upload previews to AFBlueTube and provide to social media

Coordinate release with social media team

Prepare metadata for product distro
- Write podcast description
- Create tags

5 DISTRIBUTION

Upload podcast to DVIDS

Coordinate with DVIDS to push podcast to iTunes

Make AFBlueTube podcast link public

Final hot wash & lessons learned
- After Action
- Documents added to project folder

Archive Podcast
- Save final master MP4 to AFTV archive
- Archive raw audio files, video and b-roll
- Archive all assets
- Archive all paperwork
- Archive Project Folder