ONLINE CONDUCT FOR THE NAVY TEAM

May 30, 2017

Produced by the Navy Office of Information (CHINFO)

ONLINE CONDUCT
"Honor, Courage, Commitment Online, All of the Time."

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

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

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

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

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

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

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

JOINING NETWORKS

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

SETTING GUIDELINES

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

THE UCMJ AND NAVY REGULATIONS

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

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

POSSIBLE TYPES OF LEGAL CONSEQUENCE

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

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

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

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

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

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

REPORTING INCIDENTS

Any member of the Navy community experiencing or witnessing incidents of improper online behavior should promptly report matters to their chain of command via the Command Managed Equal Opportunity (CMEO) or Fleet and Family Support Office. Additional avenues for reporting include Equal Employment Opportunity Offices, the Inspector General, DON Sexual Assault Prevention and Response offices (SAPRO), and Naval Criminal Investigative Service (NCIS).

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

Specific instructions are available at: www.NCIS.navy.mil/reportacrime

BOTTOM LINE

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

Chief of Naval Operations Adm. John Richardson

ONLINE SAFETY AND BEST PRACTICES

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

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

When you are online, you are in public … so act like it!

- *Don't do or say anything online you wouldn't do or say in public!* Keep relationships and personal life private.
- Treat everyone online how you'd like to be treated. The "Golden Rule" applies even online!

There is no such thing as complete anonymity online!

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

Before you hit send, stop and think…

- Words and things you say matter.
- Images can be taken out of context.
- Cool off before responding to messages in anger.
- You'll never agree with everyone online.
- Respect others' opinions.
- Anyone anywhere can see what you post.

*…**the Internet doesn't forget**.*

- It is very easy for bad actors to save a screenshot, download an image, or do something else to make sure a moment online lasts an eternity.
- Anything shared online, although intended to be private and confidential, has the possibility to become public – if it is best left unsaid, do not say it. **If you don't want it shared, don't post it.**
- Protect your privacy and your friends' privacy too by not sharing without their permission.
- And unless you're prepared to attach that post, text or photo to your next college application, security clearance package, or resume, again, **stop and think before you post**.

Security

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

How to be a hard target:

- **Keep your technology up to date** (computer, phone, etc.). Whenever you get a software update at work or at home, run it. These are typically patches for recent security vulnerabilities.
- **Beware of tracking your location.** Many social media platforms allow for "check in" and broadcast your location, or automatically add location information to photos and posts.
- **Stay away from public Wi-Fi**. With a public Internet connection, you run the risk of being hacked. If you must use a public Wi-Fi connection, there are some things you can do to be safer:
    - Don't shop or go to your bank accounts on public Wi-Fi.
    - Only go to sites that use a secure connection (indicated by an "HTTPS" in their web address). This means they use encryption to protect your information.
    - Use a Virtual Public Network (VPN). This is a service you pay for that gives you a secure connection wherever you are.
    - If available, use two-factor authentication. Anyone trying to pretend to be you won't be able to access your accounts because they won't have your phone or computer.
    - Set login notifications on all your accounts so when someone tries to login from a new location you get an email and can take proactive action if necessary.
- **Backup your data.** Frequently backup data at home and in the workplace. Many commercial cloud and physical storage devices will encrypt data automatically for extra protection.
- **Strong Password Protocols**.
    - The best password is a string of at least 12-15 random characters containing numbers, upper and lower case letters and symbols.
    - Don't try and remember all passwords for all platforms and devices. Use a password manager.
    - Do not share passwords.
    - Don't use the same password for more than one site or device.
    - Never reuse an old password.
    - Answer security questions creatively. Sites often have security questions of personal information to help you recover or reset a password. For example: Hackers can deduce the answers from social media accounts to make attempts at changing an individual's password, locking them out and stealing valuable data. Make this harder by either giving a different response to the question or padding your response with something no one knows but you such as adding a special character [*] at the end of a response.
    - Put passwords on all of your devices and put a strong password on your network at home. This includes changing the default password on personal routers at home.