# LIMITED PERSONAL USE OF GOVERNMENT DESKTOP EQUIPMENT, WIFI, AND MOBILE DEVICES

**COMDTINST 5375.1E**
**August 2022**

THIS PAGE INTENTIONALLY BLANK

U.S. Department of Homeland Security
United States Coast Guard

Commandant
United States Coast Guard

US Coast Guard Stop 7710
2703 Martin Luther King Jr Ave SE
Washington, DC 20593-7710
Staff Symbol: CG-62
Phone: (202) 475-3482

COMDTINST 5375.1E
05 AUG 2022

COMMANDANT INSTRUCTION 5375.1E

Subj: LIMITED PERSONAL USE OF GOVERNMENT DESKTOP EQUIPMENT, WIFI, AND MOBILE DEVICES

Ref: (a) Standards of Ethical Conduct, COMDTINST M5370.8 (series)
(b) DHS Management Directive 4600.1, Personal Use of Government Office Equipment, April 14, 2003
(c) DHS 4300A, Sensitive Systems Handbook, November 15, 2015
(d) U. S. Coast Guard Cybersecurity Policy, COMDTINST 5500.13 (series)
(e) USCG Civil Rights Manual, COMDTINST M5350.4 (series)
(f) 5 C.F.R. §§2635.703, .704, and .705, Use of Government Property
(g) Coast Guard External Affairs Manual, COMDTINST M5700.13 (series)

1. PURPOSE. This Instruction defines the policy on personal use of government office equipment and services by all Coast Guard personnel (military, civilian, and auxiliary) and contractors (under Coast Guard contract) in accordance with References (a) through (f). The use of government office equipment and services for official use is authorized for Coast Guard and authorized personnel, however is not addressed by this Instruction. This Instruction's scope does not apply to Morale, Welfare, and Recreation (MWR) equipment.

2. ACTION. All Coast Guard unit commanders, commanding officers, officers-in-charge, deputy/assistant commandants, and chiefs of headquarters directorates must comply with the policies contained in this Instruction.

3. AUTHORIZED RELEASE. Internet release is authorized.

4. DIRECTIVES AFFECTED. Limited Personal Use of Government Office Equipment and Services, COMDTINST 5375.1D, is hereby canceled.

5. DISCUSSION. Since the inception of the original policy on Limited Personal Use of Government Desktop Equipment, WiFi, and Mobile Devices, Information Technology (IT) infrastructure continues to be an integral component of daily operations and business activities in the Coast Guard. Policy on limited use is important as the aggregate use by those unauthorized could negatively impact the Coast Guard Network (CG Network).

6. DISCLAIMER. This guidance is not a substitute for applicable legal requirements nor is it itself a rule, it is intended to provide administrative guidance for personnel and is not intended to nor does it impose legally-binding requirements on any party outside the Coast Guard.

7. ENVIRONMENTAL ASPECT AND IMPACT CONSIDERATIONS. The Office of Environmental Management (CG-47) reviewed this Commandant Instruction and the general policies contained within, and determined that this policy falls under the Department of Homeland Security (DHS) categorical exclusion A3. This Commandant Instruction will not result in any substantial change to existing environmental conditions or violation of any applicable federal, state, or local laws relating to the protection of the environment. It is the responsibility of the action proponent to evaluate all future specific actions resulting from this policy for compliance with the National Environmental Policy Act (NEPA), other applicable environmental requirements, and the U.S. Coast Guard Environmental Planning Policy, COMDTINST 5090.1 (series).

8. DISTRIBUTION. No paper distribution will be made of this Instruction. An electronic version will be located in the Coast Guard Directives System Library internally, and if applicable on the Internet at www.dcms.uscg.mil/directives .

9. LOCAL RESTRICTIONS. Commanding officers and officers-in-charge may further reduce personal usage of government office equipment or services due to bandwidth restrictions as a result of increased operational tempo or degradation of network services (e.g., no attachments to e-mail authorized).

10. DEFINITIONS. The following are definitions as pertaining to this Instruction.

    a. Coast Guard Personnel. Coast Guard personnel includes military, civilian, auxiliary, and volunteer employees for purposes of this Instruction.

    b. Government Office Equipment/Services. Equipment and/or systems purchased, leased, and/or owned by the government. This includes, but is not limited to, IT equipment, (including WiFi), e-mail, library resources, telephones, portable electronic devices (PED), smartphones, facsimile machines, photocopiers, and office supplies.

    c. IT Equipment. Any equipment, interconnected systems, or subsystems of equipment thatis used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.IT equipment includes, but is not limited to, CG Standard Workstation (CGSW) desktopsor laptops, Portable Electronic Devices (PED), smartphones, related peripheral equipment, WiFi, and software.

    d. Non-Windows Operating System (OS) Devices. Cellular devices and tablets and other non-windows operating devices.

    e. Non-Work Hours. Any time Coast Guard personnel are not required to perform assigned duties. Examples of non-work hours may include, but are not limited to, scheduled lunch periods, before or after a workday, non-work weekends, and holidays.

    f. Portable Electronic Device (PED). Any non-stationary electronic apparatus with singularor multiple capabilities of recording, storing, and/or transmitting data, voice, video, or photo images (e.g., cell phones, laptops, tablets, and wearable devices such as

fitness bands, and smart watches).

g. Personal Use. Any use conducted for a purpose other than accomplishing official Coast Guard business.

h. Smartphone. A cellular telephone with built-in applications and Internet access. Smartphones provide digital voice service as well as text messaging, e-mail, Web browsing, still and video cameras, MP3 player, video viewing, and often video calling. In addition to their built-in functions, Smartphones can run a myriad of applications, turningthe once single-minded cell phone into a mobile computer.

11. PERSONAL USE POLICY.

a. Personnel must be authorized to use government office equipment or services for official government business before it is available for limited personal use.

b. Personal use of government office equipment or services is never authorized for Contractors. Contractors are restricted to the use of government office equipment and services ONLY for official business purposes.

c. Personal use of government office equipment or services is authorized for Coast Guard personnel only when such use:

(1) Does not interfere with official duties, inhibit the security of information, information systems, or cause degradation of network services;

(2) Is limited and infrequent; and,

(3) Is of nominal cost to the government.

d. Coast Guard personnel shall consult their supervisor regarding authorized use should any questions arise. Supervisors and Coast Guard personnel are expected to exercise reasonable discretion when deciding whether to use government office equipment for personal use.

e. Managers and supervisors may further limit the personal use of equipment based on the needs of the command or office.

f. Any unauthorized personal use incidents (suspected or actual) must be reported to the local/unit Information Systems Security Officer (ISSO) or Cyber Security Operations Center (C-SOC) (CGYBER-SOC@uscg.mil) including introduction of an IT virus/worm, malicious software (malware), accidental release of sensitive information, or anything that compromises the confidentiality, availability, authentication, or non-repudiation of the Coast Guard Enterprise IT inaccordance with Reference (d).

g. Users with Cloud Based Internet Isolation (CBII) installed on their CGSW may access enabled websites such as commercial email, and social medial platforms such as *YouTube*, *Facebook, Twitter, Instagram,* and *LinkedIn*, during the users' scheduled breaks.

12. PROHIBITED USE POLICY FOR GOVERNMENT FURNISHED EQUIPMENT.

a. The following in sub paragraphs 12.a. (1) through (11) is prohibited at all times on Coast Guard equipment (including during non-work hours) except for investigative purposes, or as authorized for official use by the commanding officer, officer-in-charge, or equivalent; this includes any misuse that could result in adverse administrative or criminal actions against an individual:

(1) Use of government office equipment or services to intentionally and knowingly view, download, store, display, transmit, or copy any materials that are sexually explicit, or are predominantly sexually oriented. Sexually explicit or predominantly sexually oriented includes, but is not limited to, any material that depicts, in actual or simulated form, or explicitly describes, sexual content (sexual contact, nudity, child pornography, sexting, etc.). “Intentionally” and “knowingly” may be inferred based on repeated downloading, storing, displaying, transmitting, or copying of the prohibited materials referenced in this section;

(2) Intentionally creating, copying or transmitting any materials or communications that may be considered hate incidents or discriminatory to fellow employees or to the public. Illegal discrimination is any intentional action or omission that results in the adverse treatment of a person because of that person's race, color, religion, national origin, disability, handicap, age or gender, including sexual harassment or intentional actions or omissions in reprisal. Hate incident is defined as any intentional act (conduct or speech) of intolerance committed against a person, a group of individuals,or property which is motivated, in whole or in part, by the offender’s bias against a race, color, religion, sex, national origin, disability, age, or sexual orientation and which is intended to or is more likely than not to have the effect of intimidating others or inciting others to similar conduct in accordance with Reference (e);

(3) Loading personal or unauthorized software onto a government computer or other government office equipment;

(4) Purposefully making unauthorized configuration changes to a government computer system or other government office equipment;

(5) Using government office equipment or services as a staging ground or platform to gain access to unauthorized systems;

(6) Deliberate introduction of viruses, worms, or other malicious software (malware) into the CG Network or any other government network;

(7) Intentionally and knowingly creating, copying, or transmitting SPAM, PHISHING, chain letters, or any unofficial mass mailings, regardless of the subject matter;

(8) Subscribing, downloading (movies, music, books, etc.), or enabling other automatic

Internet service(s) from a CGSW (desktop or laptop), unless specifically authorized for Coast Guard business;

(9) Intentionally and knowingly acquiring, reproducing, transmitting, distributing, or using any controlled information including computer software and/or data protected by copyright, trademark, privacy laws, or other proprietary data or material with other intellectual property rights beyond fair use, without consent or authorization of the copyright holder, or export-controlled software and/or data;

(10) Connecting personally-owned IT equipment (laptop, iPad, Tablet, Smartphone, etc.), except on an approved WiFi connection, to the CG Network at a Coast Guard office or facility without prior approval by the Coast Guard Office of Cybersecurity Program Management, Commandant (CG-62). This includes visitors (U.S. Citizens or Foreign Nationals), contractors, vendors, other government agencies, or non-Coast Guard employees; and,

(11) Misuse of sensitive information including the intentionally creation, copying, or transmitting any materials or communications such as classified, FOUO or other sensitive information.

13. INAPPROPRIATE USE POLICY.

a. Unless when expressly authorized for official purposes, the following in sub paragraphs 13.a. (1) through (5) includes actions considered inappropriate. Any violations of the inappropriate use portion of this Instruction could result in administrative and/or disciplinary action against military and civilian personnel. Contractor personnel who violate this policy may be released for cause. Actions inappropriate are as follows:

(1) Using a Coast Guard e-mail address (e.g. First.M.Last@uscg.mil) for subscribing to anything other than official, professional, or job-related websites;

(2) Engaging in any fundraising activity not sanctioned by the Coast Guard, endorsing any non-Federal Government organization or service, and engaging in any political activity;

(3) Using government office equipment or services for commercial purposes to support a private or personal business, including assisting relatives, friends, or other persons in such activities. Examples of this prohibition include, but are not limited to, employees using a government computer and Internet connection to run a travel business, investment, or consultant service;

(4) Using government office equipment or services for private, non-profit, non-commercial business or activities. Examples of this prohibition include, but are not limited to, organizing charity event participation and soliciting volunteers for non-Coast Guard sanctioned activities; and,

(5) Use of government office phones, cellular, or Smartphone devices that could incur unnecessary government expenses, unless specifically related to the Coast Guard

mission (e.g., long distance charges, roaming charges, International charges, data charges, additional minutes, etc.).

14. EXCEPTIONS.

a. Exceptions to the prohibited and inappropriate uses shall be in accordance with the following:

(1) Use of Smartphones and tablets shall be in accordance with the Wireless Mobile Device User Agreement, Form CG-5233;

(2) The Coast Guard Director of Government and Public Affairs, Commandant (CG-092), and Coast Guard External Affairs Manual, COMDTINST M5700.13 (series) for public and social media websites; and,

(3) If using an "USCG.MIL" email account for professional or job related (non-federal program) reasons, a CG member, employee, or contractor must not give the appearance that the United States Coast Guard endorses or sanctions that individual's personal activities. If there is potential for confusion, employees must provide an appropriate disclaimer such as: "*The content of this message does not reflect the official position of the United States, the Department of Homeland Security (DHS), or the United States Coast Guard*."

b. Personal Devices on Government Furnished Commercial WiFi:

(1) CG provided Commercial WiFi use is authorized for personal use on personal time (before and after work; during lunch and other breaks. Personal devices may be used to infrequently check emails, pay bills, etc. Personal devices may also be used to watch Coast Guard approved streaming videos from the #CGHOWTO and *MilTube* video library and make video/telephone calls to communicate with family and friends provided there is no additional direct cost to the Government. The following activities are absolutely prohibited on any government furnished WiFi system:

(a) Gambling;

(b) Visiting and/or downloading material/content from pornographic websites;

(c) Lobbying. This includes U.S. Congress or any government agency. Note, this prohibition does not include activities protected by Whistleblower statutes or contacting government agencies to resolve personal issues such as renewing a driver's license, resolving a tax issue, communicating about a student loan issue, etc.;

(d) Campaigning or political activity. This does not include registering to vote, requesting an absentee ballot, or voting, etc.;

(e) Endorsements of any products, services, or organizations in your official

capacity;

(f) Fundraising for external organizations or purposes (except as required as part of your official duties under applicable statutory authority and agency policy) in your official capacity; and,

(g) Any type of continuous audio or video streaming from commercial, private, news, financial organizations.

(2) The use of WiFi is not authorized for any personal use that could cause congestion, delay, or disruption of service to any government system or equipment (i.e., sending video, sound or other unofficial large file attachments, and any high bandwidth related activities such as gaming, streaming, and listening to radio stations).

(3) Photos, videos, and non-public releasable information must not be posted on social media websites, this is not authorized; and,

(4) Location information must be disabled while GFE WiFi is being used on personal devices.

c. Government Mobile Devices:

(1) Government accounts must be accessed by using GFE or on non-GFE equipment through an approved CG solution for remote work, such as VDI or VPN;

(2) Users whose devices are managed by Intune should download mission related apps from the Comp Portal. Users may use their personal email to obtain an Apple ID, and download personal apps from the Apple App Store for limited, infrequent use as outlined in this policy; and,

(3) Upon request, additional mission related mobile apps may be added to the Comp Portal with a mission related justification. To request an app be approved for CG mobile devices for official use, submit your request via the Coast Guard Office of Command, Control, Communications, Computers (C4) and Sensors Capabilities, Commandant (CG-761) C5I intake tool located at: https://cg.portal.uscg.mil/units/cg761/requirements/intake/SitePages/Home.aspx .

15. DEPLOYED UNITS. Bandwidth, at times, may be extremely limited for underway, forward deployed, and isolated units. Commands shall manage bandwidth, as an asset, to meet both mission requirements and to support unit morale. Commands are authorized to approve personal use on a case-by-case-basis.

16. RECORDS MANAGEMENT CONSIDERATION. Records created as a result of this Instruction, regardless of format or media, must be managed in accordance with the records retention schedules located on the Records Resource Center SharePoint online site: https://uscg.sharepoint-mil.us/sites/cg61/CG611/SitePages/Home.aspx .

17. FORMS/REPORTS. The forms referenced in this Instruction are available on the Coast Guard Standard Workstation or on the Internet: www.dcms.uscg.mil/Our-Organization/Assistant-

Commandant-for-C4IT-CG-6/The-Office-of-Information-Management-CG- 61/Forms-Management/ .

18. SECTION 508. This Instruction was created to adhere to Accessibility guidelines and standards as promulgated by the U.S. Access Board. If changes are needed, please communicate with the Coast Guard Section 508 Program Management Office at: Section.508@uscg.mil.

19. REQUEST FOR CHANGES. Commandant (CG-6) will coordinate the promulgation of time-sensitive amendments when needed. Recommendations for improvement or corrections should be submitted directly to Commandant (CG-62).

/CHRISTOPHER. A. BARTZ/
Rear Admiral, U.S. Coast Guard
Assistant Commandant for C4IT (CG-6)