



DEPARTMENT OF THE NAVY

NAVAL ACADEMY PREPARATORY SCHOOL
440 MEYERKORD AVENUE
NEWPORT, RI 02841-1519

NAPSINST 5230.1
9 Aug 18

NAVAL ACADEMY PREPARATORY SCHOOL INSTRUCTION 5230.1

From: Commanding Officer, Naval Academy Preparatory School

Subj: POLICY FOR USE OF COMPUTER AND TELECOMMUNICATIONS
RESOURCES

Ref: (a) USNAINST 5230.1C

Encl: (1) Student Custody Agreement

1. Purpose. To establish a policy to ensure the proper use of Naval Academy Preparatory School (NAPS) computer and telecommunication resources and services by military and civilian employees, independent contractors, students, and other computer users. All computer users have the responsibility to use computer resources in an efficient, effective, ethical, and lawful manner. This policy is provided to augment reference (a) and all directives and instructions already in place as provided by the Department of Defense, Department of the Navy, U.S. Naval Academy (USNA) and other instructions and directives. The guidelines presented herein do not cancel or supersede any of these existing documents and is provided only to amplify those requirements.

2. Cancellation. NAPSINST 2300.1G

3. Discussion.

a. The following policy, rules, and conditions apply to all users of computer and telecommunication resources and services, wherever the users are located. Violations of this policy may result in disciplinary action, including non-judicial punishment, Midshipman Candidate expulsion, employee termination, and/or corresponding legal action.

b. NAPS has the authority, to monitor any and all aspects of the computer system, including employee data files and e-mail, to ensure compliance with this policy. The computers and computer accounts given to employees are to assist them in the performance of their duties. Personnel should not have an expectation of privacy in anything they create, send, or receive on their assigned computer or while using NAPS computer resources. Computer and telecommunication systems at NAPS belong to the U.S. Government and may be used for official purposes only. Personal e-mail messages may be sent and received so long as these messages are conveyed in a professional manner. All information must reflect the highest standards of moral, ethical and legal communication.

c. All NAPS personnel are governed by the following provisions, which apply to the use of all computer and telecommunication resources and services. Computer and

9 Aug 18

telecommunication resources and services include, but are not limited to the following: host computers, file servers, workstations, standalone computers, laptop computers, software, network wiring, connecting equipment, and internal or external communications networks (Internet, commercial on-line services, bulletin board systems, and e-mail systems) that are accessed directly or indirectly from NAPS computer facilities.

d. This policy may be amended or revised periodically as the need arises.

e. The term "users," as used in this policy, refers to all military and civilian employees, independent contractors, students, and other persons or entities accessing or using NAPS computer and telecommunication resources and services.

f. The term "computer(s)," as used in this policy, refers to desktop computer models and laptop models unless specifically stated as such.

g. This policy should be interpreted to encompass not just the specific regulations but also the overall spirit that this document is intended to embody. As an aid to that interpretation, the following regulations are provided as specific guidelines:

(1) Users are responsible for taking reasonable safeguards to protect and preserve any government issued computer, or information technology equipment (i.e. docking station, monitor, keyboard or mouse). Unless a laptop is being moved from one location to another it should remain attached to a docking station. When a laptop is removed from a docking station and is carried to another location, such as from Ripley Hall to Perry Hall, it will be stowed in a NAPS-issued carrying case. Do not use backpacks to transport laptops. Laptops may be used in an assigned room/office, Ripley Hall common areas, NAPS labs (Chemistry or Physics), classrooms, or academic offices. Laptops are not to be removed from the NAPS campus area without specific permission granted by the chain of command. Users will be held financially liable for any lost laptops or any damage due to negligence. The cost to replace a lost or non-repairable laptop is \$1,400.

(2) Users may not attach or electrically connect any device, digital or otherwise, to any NAPS computer, or information technology equipment, either internally or externally, without the express permission of NAPS IT personnel. This includes external storage media of any kind, e.g., flash drives, thumb drives, digital cameras, music players, printers, router, tablet, external hard disk drive or cell phones. Additionally, users may not attach or electrically connect any component or subcomponent of a NAPS computer to any other device except as specifically authorized by NAPS IT personnel. This includes but is not limited to use of a computer monitor attached to a television, movie or game device. Similarly, users may not utilize any part of the NAPS network infrastructure, including wiring, Ethernet switches, hubs, or servers to play games, display video information (streaming video such as Netflix, Amazon Prime, YouTube Red and other movie services), play music or otherwise communicate using personal electronic equipment, computer, or game device. The Go WIFI commercial service in Ripley Hall is not authorized for use on government issued laptops and is blocked.

9 Aug 18

(3) Users must comply with all software licenses, copyrights, and all other state and federal laws governing intellectual property. As such, no user shall install, copy, or otherwise use any software or application program that is not provided by the NAPS Information Technology branch without the express permission of NAPS IT personnel. Failure to comply with software licensing and other intellectual property laws can constitute a felony and can be prosecuted as such.

(4) Fraudulent, harassing, embarrassing, indecent, profane, pornographic, obscene, intimidating, or other unlawful or disreputable material may not be sent by e-mail or other form of electronic communication. Likewise, this type of material may not be accessed, displayed on or stored on NAPS computers. Users encountering or receiving such material should immediately report the incident to their supervisor.

(5) NAPS will fully support the policies of the U.S. Navy with regard to discrimination, sexual harassment, hazing and sexual misconduct. To this end, using NAPS computers, or infrastructure to access or transmit any questionable material such as, but not limited to, extremist sites, modeling or "bikini" pictures, celebrity sites, and band or song lyric sites, etc., is deemed "gray area" information. All users must be aware that internet sites containing this gray area type of information are known to carry automatic advertisements, links, and pop-up references and redirections to disreputable, pornographic, or otherwise objectionable material on the Internet. Consequently, all users will be responsible for all access from their LAN account that are spawned or propagated from these gray area sites, whether or not the access was intentional. Further, it will not be the responsibility of NAPS IT personnel to investigate such access, except to report the access as internet abuse, or to assist in conducting investigations as requested by the command.

(6) Users should use the same care in drafting e-mail and other electronic documents as they would for any other written communication. Anything created on the computer or laptop may be, and likely will be, reviewed by others. Any communication is a reflection on the individual, NAPS, the Department of the Navy and the U.S. Government. As such, and as a keeper of public trust, great care must be used to convey a positive appearance and impression on any reader.

(7) Users may not download or install any program, application, utility, game or other software onto government-owned computers, or the NAPS network without first receiving explicit authorization to do so from NAPS IT personnel. This includes software known as "freeware," "shareware," "demo," or other similar programs.

(8) Users may not use any peer-to-peer (P2P) service such as uTorrent, Bit Torrent, Pando or web based service such as iTunes.com, Amazon.com and Sony.com to download music or any other files to a NAPS computer or laptop.

(9) Users may not use any computer, or the NAPS infrastructure to play any game, installed or via the Internet, without first receiving explicit authorization to do so from NAPS IT personnel. Likewise, use of any computer or telecommunication resource to participate in any wagering or gambling activity is strictly prohibited. Additionally, accessing or attempted access

9 Aug 18

to any video game related site is prohibited. These include, but are not limited to, Internet sites that allow on-line game play, game reviews, game downloads, and game "cheat code" information or "tips."

(10) Users may not alter or copy any file belonging to another user without first obtaining permission from the owner of the file. The ability to read, alter, or copy a file belonging to another user does not imply permission to read, alter, or copy that file.

(11) Without prior specific permission, the computer and telecommunication resources and services of NAPS may not be used for the general transmission or storage of commercial or personal advertisements, solicitations, promotions, or political or religious material.

(12) Destructive or "nuisance" programs (viruses and/or any self-replicating or mutating code) will not be authored, intentionally transmitted or stored on any NAPS computer.

(13) Users may not create, transmit, forward or propagate any e-mail messages designed to solicit or induce any other person to forward the message in kind to others, typically referred to as "chain mail" or "chain letter e-mail."

(14) Users may not use any e-mail function to intentionally send multiple copies of the same e-mail message to any individual or group within or outside of NAPS. Attempts commonly called "flooding" or "bombing," or any other distribution of excess e-mails, is specifically prohibited. This includes practical jokes as well as vengeance or harassing e-mail intended to result in delivery of numerous messages to overload a mail server, service or individual mailbox/account.

(15) Users may not use NAPS computers or telecommunications infrastructure to join, receive, participate in, or otherwise communicate using Internet sites or software designed for group or social communication, better known as forums, "blogs," "chatting," "voice over IP," or "instant messaging" unless specifically required and authorized by NAPS IT personnel for NAPS business purposes.

(16) Users are responsible for safeguarding their passwords for the system. Individual passwords should not be printed, stored on-line, or given to others. Users are responsible for all transactions made using their accounts/passwords. Likewise, users will be responsible for Internet site access resulting from "pop-up" pages if using email accounts other than their NAPS provided account. Users should be suspicious and cautions when opening mail as well as unfamiliar web pages.

(17) A user's ability to connect to other computer systems through the network does not imply a right to connect to those systems or to make use of those systems unless specifically authorized by the operators of those systems. Likewise, the ability to access any site on the Internet does not imply that the user is authorized to view or otherwise access the site and all access is still restricted as identified within this instruction.

(18) "Hacking" or deliberately attempting to infiltrate or bypass any security or

9 Aug 18

administrative measure (software or hardware) to obtain access to any disk area or file on any NAPS server, computer, or to any Internet site is expressly forbidden. Likewise, users are not permitted to make any configuration changes to their computer that are not authorized by NAPS IT personnel. Students are not authorized to make any change to computer configurations as setup by NAPS IT personnel, including but not limited to, network settings, Internet settings, or network drive mappings.

(19) Users are responsible for taking reasonable safeguards to protect and preserve any issued computer or Information technology equipment. Further, no computer equipment shall be left energized or operating while in a closed locker, desk, or cabinet unless in compliance with the express directions of NAPS IT personnel.

(20) NAPS is not responsible for the actions of individual users. As such, NAPS is not liable for any actions taken by any individual against any other individual, computer or computer system except as provided for by higher authority within the Department of the Navy or Department of Defense.

4. Responsibility.

a. The NAPS Information Technology branch head is responsible for the establishment, definition and interpretation of this instruction as well as applying and interpreting other applicable guidelines concerning information technology equipment and infrastructure.

b. Under guidance of the Information Technology branch head, NAPS Information Technology personnel are responsible for assessing NAPS computer and telecommunication access processes, implementing and administering access policies, rules and restrictions as needed to maintain and protect the integrity of this instruction and the NAPS computer and telecommunication systems infrastructure. In addition, the Information Technology Branch is responsible for monitoring and reporting abuses of this instruction or other NAPS regulations as required.

c. Department heads and supervisors are directed to ensure awareness of this policy by all personnel at NAPS including any persons given access to NAPS computer and telecommunications resources from within or outside of this command.

d. All midshipman candidates will sign enclosure (1) upon issuance of IT equipment.

e. All users of computer and telecommunications resources at NAPS are directed to comply with these guidelines as well as the spirit in which they are presented.


C. R. HOWES

9 Aug 18

Student Custody Agreement

All computers have a seven digit barcode number on a Property of U.S. Navy sticker found on the top of the computer. All monitors also have a seven digit barcode number on a Property of U.S. Navy sticker found on the back of the monitors. Use these numbers to fill out the top part of this form.

Last Name			
Alpha Code			
Room Number		Which side of room as you walk in door? Circle one: Port Starboard	
Computer Barcode		Monitor Barcode	

Custody Agreement

By accepting custody, I agree to abide by all DOD and DON policies regarding the use of NAPS computer equipment. Damage to computer equipment due to negligence is subject to punishment under the NAPS conduct system or the UCMJ.

Place a check mark in each box below after reading the Policy for use of Computer and Telecommunications Resources. This policy can be found by clicking on the NAPS Intranet icon on Student Menu window.

- I have read the Policy for use of Computer and Telecommunications Resources.
- I will not make any software or hardware configuration changes.
- I agree that I will not connect any device to my NAPS issued computer, such as phone, printer, hard drive, access point or any USB device.
- I agree that when transporting my government issued laptop I will use the carrying case that was issued to me.
- I agree that will only connect my Government issued laptop to Government network(s).
- I have enrolled in Password Portal.

Student's Signature

Date

