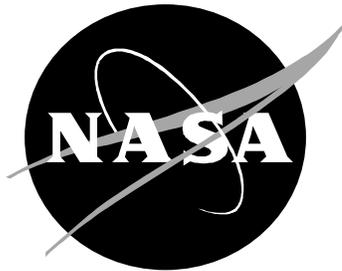


Interim NASA Headquarters Information Technology Policy



Effective Date: December 23, 2008
Expiration Date: December 23, 2009

**NASA Headquarters Appropriate Use of Information Technology
Resources**

**Responsible Office: LM020 – Office of Institutions and Management, Office of
Headquarters Operations, Headquarters Information Technology and
Communications Division**

National Aeronautics and
Space Administration

Headquarters
Washington, DC 20546-0001

Reply to Attn of: **Headquarters Information Technology & Communications Division**

TO: All NASA Headquarters Employees & Contractors

FROM: Acting Director, Headquarters Information Technology and Communications
Division

SUBJECT: Policy on Appropriate Use of NASA Headquarters Information
Technology Resources

In my capacity as the NASA Headquarters Chief Information Officer (CIO), I am transmitting the updated policy on appropriate use of NASA Headquarters Information Technology (IT) resources by way of the enclosure. It is in accordance with the guidance on appropriate use of IT resources provided in NPR 2810.1a and NPD 2540.1F as well as the recommended guidance developed by the Federal CIO Council. However, it also provides additional guidance and tailoring for the NASA Headquarters environment.

The enclosed policy is applicable to all NASA Headquarters Civil Service and contractor employees and all other individuals authorized to use NASA Headquarters IT resources.

If you need additional information regarding the Headquarters IT usage policy, please contact me at 358-7220. To obtain assistance with related legal questions, consult the Headquarters Office of the General Counsel. For matters regarding IT Security, consult the Headquarters IT Security Manager at 358-2218.

Victor L. Thompson

Enclosure

TABLE OF CONTENTS

TABLE OF CONTENTS	i
1. POLICY	1
2. APPLICABILITY	1
3. AUTHORITY	2
4. REFERENCES	2
5. RESPONSIBILITY	2
6. DELEGATION OF AUTHORITY	3
7. MEASUREMENTS	3
8. CANCELLATION	3
APPENDIX A - REQUIREMENTS	4
A. Official Business and other Authorized Activities	4
B. Personal Use	4
C. Inappropriate Use	5
D. Protecting IT Resources	8
E. Authorized At Home Use of NASA IT Resources	9
F. Proper Representation	9
G. Privacy Expectations	10
H. Sanctions for Misuse	10
APPENDIX B – QUESTIONS & ANSWERS	12
APPENDIX C - ABBREVIATIONS	15

Appropriate Use of NASA Headquarters Information Technology Resources

1. POLICY

This document establishes NASA Headquarters (HQ) policy and responsibilities for employee appropriate use of NASA HQ Information Technology (IT) resources. NASA HQ IT resources are essential tools for communications, research and analysis, collaboration, ongoing operations, and other work performed at NASA HQ. Employees are encouraged to develop their expertise and make full use of these valuable Government assets to effectively accomplish their official duties. Because modern information technology provides new opportunities for people everywhere to live their lives more efficiently, NASA HQ employees are allowed limited personal use of government provided IT resources. This is in accordance with the trust relationship between NASA HQ and its employees and the NASA goal of providing a modern, productive, and supportive work environment.

NASA HQ IT resources are primarily for official business and other authorized activities. A limited amount of personal use of NASA HQ IT resources is permitted provided it meets the following requirements:

- Does not interfere with NASA missions or operations.
- Does not affect employee productivity
- Does not incur any additional expense to the Government.
- Is not illegal or inappropriate.
- Does not violate the Standards of Ethical Conduct for Employees of the Executive Branch (5 CFR 2635).

NASA HQ IT users need to be aware of the fact that there is no expectation of privacy at any time. Monitoring of systems may be conducted at any time to ensure the integrity, availability, and confidentiality of the systems and the data they contain.

2. APPLICABILITY

This policy sets forth NASA HQ policy and responsibilities for the appropriate use of NASA IT resources. IT resources include computers, networks, software, peripheral equipment, Internet services, electronic mail, facsimile machines, pagers, and personal digital assistants. This policy does not address appropriate use of telephones or photocopiers. See NASA Program Directive (NPD) 2540.1F, Personal Use of Government Office Equipment including IT and NASA Program Requirement (NPR) 1490.1G, NASA Printing, Duplicating, and Copying Management for information on these devices.

This policy is applicable to all NASA HQ government employees, contractors, consultants, and all other individuals authorized to use NASA HQ IT resources. All of the privileges and prohibitions herein apply to both onsite and offsite (e.g., at home or on travel) usage of HQ IT resources.

3. AUTHORITY

NPR 2810.1A, Security of IT, May 16, 2006, grants the Center Chief Information Officer (CIO) the authority to establish Center policies and procedures to ensure the secure operation of Center systems and the protection of Center data and information.

4. REFERENCES

- a. NPR 2810.1A, *Security of Information Technology*, May 16, 2006
- b. NPD 2540.1F, *Personal Use of Government Office Equipment Including Information Technology*, May 25, 2005
- c. NPR 1490.1G, *NASA Printing, Duplicating, and Copying Management*, January 12, 2006
- d. 5 CFR 2635, *Standards of Ethical Conduct for Employees of the Executive Branch*
- e. Office of Management and Budget (OMB) Memorandum M-04-26, *Personal Use Policies and File Sharing Technology*, September 8, 2004
- f. General Services Administration (GSA) Office of Government-wide Policy Memorandum, *Model "Limited Personal Use Policy" of Government Equipment*, June 7, 1999
- g. NPR 1450.10D, *NASA Correspondence Management & Communications Standards and Style*, March 24, 2006
- h. NPR 1441.1D, *NASA Records Retention Schedules (w/Change 4, 1/31/2008)*, February 24, 2003

5. RESPONSIBILITY

The HQ ITSM shall

- Ensure that all NASA HQ IT Resource users are familiar with their responsibilities to utilize those resources appropriately.
- Ensure that NASA HQ IT resources are appropriately monitored to detect inappropriate activities.
- Lead the investigation of inappropriate activities when detected.
- Coordinate with Office of the Inspector General Computer Crimes Division, HQ Human Resources Management, and the Office of Security and Program Protection, as appropriate, when inappropriate activities are detected.

All HQ IT Resource Users shall:

- Only use NASA HQ IT resources for official business and other authorized purposes.
- Be aware that there is no expectation of privacy at any time on NASA IT systems.
- Ensure they are familiar with IT resource prohibited practices.
- Avoid any action that could compromise the security of NASA HQ IT resources as well as the information or data that they may contain.
- Encrypt all sensitive information, using NASA approved encryption software, when transmitting it or when storing it on portable devices or storage media.

6. DELEGATION OF AUTHORITY

None

7. MEASUREMENTS

None

8. CANCELLATION

This document supersedes and cancels *NASA Headquarters Appropriate Use of Information Technology Resources Policy*, May 26, 2000.

Victor L. Thompson
NASA Headquarters Acting Chief Information Officer

Date

APPENDIX A - REQUIREMENTS

A. Official Business and other Authorized Activities

Official business can broadly be defined as any use of NASA HQ IT resources that is required to be performed as part of an employee's position at NASA HQ. This includes, but is not limited to the following:

- Work-related duties in position descriptions and performance plans.
- Work involved in special assignments.
- NASA-sponsored professional training and class work.
- Tasks directed via NASA contracts.
- HQ-authorized activities.

Certain other activities are also considered to be within the scope of official business. For example electronic mail (E-mail) used to distribute information about the following:

- Work-related events such as technical symposia, conferences, and presentations.
- HQ sponsored initiatives such as multicultural events, carpools, and Exchange Council activities.
- HQ Office specific initiatives such as Small Business Awards and Office of Space Operations Space Flights Awards.
- HQ supported activities such as blood drives, sports events, associations, and organizations.

Employees should direct questions concerning what may be considered official business, regarding NASA HQ IT resources, to their supervisor. Upon supervisor request, the Office of Headquarters Operations will provide further guidance as required.

B. Personal Use

This policy continues allowance of a **limited** amount of personal use of IT resources by HQ employees. Such personal use must be kept to a minimum. It must not interfere with official business and/or accomplishment of Agency missions nor may it incur more than minimal additional expense to the government. Personal use must not affect the employee's productivity. Personal use shall occur on the employees own time; such as before and after work, during the lunch period, or at other times as determined by NASA Management. Employee use of NASA IT resources, whether official or personal, shall not violate the Standards of Ethical Conduct for Employees of the Executive Branch (5 CFR 2635).

Authorized personal use of HQ IT resources includes brief, occasional use of electronic mail, instant messaging, and Internet services, as well as other IT resources specified herein. For example, employees may:

- Exchange brief E-mail or instant messages – Employees may occasionally send brief personal e-mails or instant messages provided they do not violate the standards of conduct. Allowable examples include replying to a greeting from a colleague or checking on a home or auto repair.
- Make limited use of Internet services – Employees may browse the Internet provided doing so does not violate standards of conduct or incur any additional expense to the Government. Allowable examples include checking the status of their personal investments (but not buying and selling of securities), seeking other employment, communicating with a volunteer charity organization, or reading news headlines.
- Use office software such as a word processing or calendaring package – Allowable examples include writing a brief note or entering a personal medical appointment on your calendar.
- Send or receive a short fax – Transmission of a short personal fax message is permitted provided doing so will not incur long distance charges.
- Use a computer printer to print out a few pages of material – Employees may print a copy of an article of purely personal interest.
- Occasionally use pagers or Personal Digital Assistant (PDA) – Employees may occasionally use their Government issued pagers or PDA's to notify a family member or colleague upon short notice that a personal appointment must be cancelled.

Employees' personal use of HQ IT resources is limited to those situations where (1) NASA is already providing equipment or services; and (2) the employee's use of such equipment or services will not result in any additional expense to NASA beyond normal wear and tear or the use of small amounts of electricity, ink, toner, or paper. NASA HQ will not install or allow installation of additional hardware or software strictly for personal use.

NASA HQ is continuing the opportunity for its employees to use IT resources for personal use in an effort to maintain a supportive work environment. However, this policy does not create the right to use government IT resources for non-government purposes. Thus, this privilege may be revoked or limited at any time by NASA HQ Officials.

C. Inappropriate Use

Employees are expected to conduct themselves professionally in the workplace and to refrain from using Government IT resources for activities that are inappropriate. Employees should

direct specific questions regarding the appropriate use of HQ IT resources to their supervisor. HQ employees are specifically prohibited from using HQ IT resources for the following:

- Any personal use that could cause congestion, delay, or disruption of service to any Government system or equipment.
- Any personal use that could result in more than minimal additional expense to the Government or that interferes with the employee's work or the work of others.
- Any activity or exchange which would violate federal, state, or local laws, regulations, or policies.
- Operating a private business, consulting, or the selling of goods and services. Employees are prohibited from using a government computer and Internet connection to run a private enterprise (such as a travel business, investment service), do consulting work for another employer, or for selling personal items on e-Bay or similar services. This prohibition also includes employees using such resources to assist relatives, friends, or other persons in such activities.
- Engaging in any outside fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity.
- The creation, downloading, viewing, storage, copying, or transmission of sexually explicit materials.
- The creation, downloading, viewing, storage, copying, or transmission of materials related to illegal gambling, illegal weapons, terrorist activities, controlled substances, and any other illegal activities or activities otherwise prohibited. This includes using Government IT resources for playing or participating in on-line gambling or lotteries.
- The creation, copying, transmission, or retransmission of chain letters or other unauthorized mass mailings regardless of the subject matter.
- Activities that are in any way inappropriate or are illegal, unethical or offensive to fellow employees or the public. Such activities include, but are not limited to hate speech or material that ridicules or disparages others based on race, national origin, gender, sexual orientation, age, disability, or religion.
- Circumventing IT security measures by actions such as removing or disabling virus detection software or attempts to deprive authorized users access to a resource. This also includes attempts to prevent or interfere with downloads, pushes, or updates to software products.

- Illegal or unauthorized entry into or modification, destruction, manipulation, or denial of access to information residing on ANY information system.
- Downloading, installing, or running security programs or utilities that may expose or exploit any weaknesses in system security, without written permission of the HQ IT and Communications Division. Prohibited programs include, but are not limited to sniffers, scanners, and password cracker programs.
- Posting Agency or any other Official or Proprietary information to external newsgroups, bulletin boards or other public forums without authority. This includes any use that could create the perception that the communication was made in one's official capacity as a Federal Government employee, unless appropriate NASA approval has been obtained. It also includes any use at odds with NASA's mission or positions. Employees should be aware that when using the Internet, an electronic "footprint" (the suffix "nasa.gov") is left behind indicating that a NASA employee was there. The "nasa.gov" Internet address is a representation of the Agency, analogous to the use of NASA letterhead, in which the opinions expressed reflect on NASA. Adding a disclosure statement that the views expressed do not represent those of the Agency or the Federal Government is not an acceptable alternative.
- The use of a NASA computer system in any way that might be interpreted as an attempt to influence a Member of Congress to favor, adopt, or oppose, by vote or otherwise, any legislation, law, policy, or appropriation of Congress. This does not prevent employees from communicating with the Congressional Branch, through proper official communication channels, for the efficient conduct of official public business. Similarly, it does not prevent employees from responding to an official request for information by a Member of Congress or their staff.
- The installation of hardware or software, to include moves, additions, alterations, deletions, or replacement of Any HQ computers, cable plant, or any other IT resource, unless specifically authorized by the HQ IT and Communications Division.
- The unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information or software. Controlled information includes, but is not limited to Sensitive but Unclassified (SBU) information, Privacy Act information, Personally Identifiable Information (PII), copyright or trademark material, Proprietary Information, Scientific and Technical Information (STI), Export Controlled Information as defined by the International Traffic in Arms Regulation (ITAR) or the Export Administration Regulation (EAR), or any other material or information with intellectual property rights (beyond fair use).
- The use of "Push" technology to send non-official information to others. This is an Internet technology that allows information to be delivered or "pushed" directly to a user who subscribes to it, rather than the user having to go look for the information on

an Internet site. The receipt of pushed information, such as school closings or severe weather alerts, is permissible provided no installation of special software is required.

- The unauthorized acquisition, installation, use, reproduction, transmission, or distribution of peer-to-peer (P2P) file sharing applications such as, but not limited to KaZaA, Gnutella, Morpheus, and LimeWire.

D. Protecting IT Resources

Employees must protect NASA HQ IT resources. Passwords must be safeguarded from any form of disclosure. Employees must also avoid any action that could compromise the security of NASA HQ computer systems or networks as well as the information and data they contain.

Employees should safeguard sensitive NASA information by only storing such data on systems specifically approved for that purpose. Employees must also ensure that sensitive information is properly encrypted, using NASA approved data encryption software, when stored on portable devices or storage media, or when electronically transmitted through the public domain. Sensitive information includes SBU, PII, STI, ITAR/EAR information, or any other information that has not been approved for public release. Sensitive information must also be properly encrypted when stored on portable devices (laptops, PDA's, or Portable Hard Drives) or storage media (memory sticks, CD-ROM's, DVD's etc).

Employees should report IT security weaknesses, incidents of possible misuse, or suspected security violations to the IT Help Desk. This can be accomplished by submitting a ticket at <https://www.odin.lmit.com/hq/hqhelpdesk.html> ; sending an e-mail to service@hq.nasa.gov ; or phoning 202-358-HELP or 866-462-7247 (toll free).

Laptop computer users need to ensure that their anti-virus software is kept current. Laptop computer users with wireless capability need to ensure that simultaneous use of wireless communications and NASA HQ wired network on the same device does not occur. Laptop computer users should always utilize Virtual Private Network (VPN) software when remotely accessing HQ resources. Contact the ODIN Help Desk for more information on these services at (202) 358-HELP or 866-462-7247 (toll free).

Full NASA guidance on IT Security is contained in NPR 2810.1A, Security of IT, May 16, 2006. This document can be found on the NASA On-Line Directive Information System (NODIS) at: http://nodis-dms.gsfc.nasa.gov/restricted_directives/displayDir.cfm?Internal_ID=N_PR_2810_001A_&page_name=main .

Employees should contact the HQ IT Security Manager (202-358-2218 or 202-358-0654) regarding any questions or uncertainties pertaining to HQ IT Security policy.

E. Authorized At Home Use of NASA IT Resources

NASA HQ provides software exclusively for use by employees in performance of their official duties. However, the license agreements of some NASA HQ software may allow it to be provided to federal employees for use on their home computer. That is, a copy may be legally taken home by employees for their personal use on their home computer. When this is done, the following conditions must be met:

- Installations of such copies are made in accordance with all applicable software licensing laws and agreements with the software vendor (e.g., a copy can be installed on only one home computer).
- The employee adheres to established rules, procedures, and guidelines for handling the software transfer media (e.g., compact disc).
- All such installed copies must be removed if the employee terminates his or her employment with NASA HQ.

Complete information on Software for Home Use can be found at http://www.hq.nasa.gov/itcd/software_home-use.html .

F. Proper Representation

It is the responsibility of employees to ensure that they are not giving the false impression that they are acting in an official capacity when they are using HQ IT resources for personal use. The Standards of Ethical Conduct for Employees of the Executive Branch (5 CFR 2635.702(b)) states:

"...an employee shall not use or permit the use of his Government position or title or any authority associated with his public office in a manner that could reasonably be construed to imply that his agency or the Government sanctions or endorses his personal activities..."

- If there is an expectation that such a personal use could be interpreted as occurring on behalf of NASA, then an adequate disclaimer must be clearly stated. One acceptable disclaimer is:

"The contents of this message are mine personally and do not reflect any position of the U.S. Government or NASA."

Employees wishing to express personal opinions in conflict with official Agency policy, missions, or positions shall not utilize Government IT resources to do so. The inclusion of a disclaimer does not change this position.

- Proper representation also extends to the official use of HQ IT resources. Employees must exercise prudent judgment when tailoring HQ IT resources to include personal preferences. NPR 1450.10D, NASA Correspondence Management & Communications Standards & Style, states that personalized signature blocks in electronic communications should only reflect official business information such as name, title, organization, telephone number, and fax number. Other information included with one's electronic mail signature is not appropriate for NASA business correspondence.
- Employees must also exercise extreme care to avoid the appearance of a relationship between NASA official business and personal activities where government IT resources are used. For example, establishing a link from an official NASA web site to an employee's personal web site is inappropriate and prohibited.

G. Privacy Expectations

Since NASA HQ IT resources are provided to support the work and missions of NASA, employees do not have a right, nor should they have an expectation, of privacy at any time while using Government IT. This includes while accessing the Internet or using e-mail. HQ employees should avoid using HQ IT resources for personal purposes to the extent that they wish their private activities to remain private. By using HQ IT resources, employees grant their consent to disclosing the contents of any files or information maintained or passed-through HQ IT resources. By using HQ IT resources, HQ employees consent to monitoring and recording of their activities.

HQ system managers and the HQ IT Security Team routinely employ monitoring tools to track system performance and to detect improper use of HQ IT resources. HQ Officials (i.e., line managers, designated representatives of the HQ CIO or IT and Communications Division, Human Resources Division, Office of Security and Program Protection, Office of the General Counsel, and the Office of Inspector General) may initiate additional monitoring any time evidence of apparent misuse or possible criminal activity has been reported or detected. This monitoring may include traffic analysis (i.e., source and destination of electronic communications to and from an employee's workstation), keystroke monitoring, examination of log files, and examination of any or all files (including e-mail) on HQ servers or workstations to the maximum extent permitted by law and NASA directives. HQ Officials may access and examine files in an employee's accounts without prior consent or notification of the individual. Employees should be aware that HQ Officials may also be required, under certain circumstances, to provide electronically stored information to outside parties such as law enforcement officials.

H. Sanctions for Misuse

Unauthorized or improper use of NASA HQ IT resources, by employees or contractors, could result in any or all of the following actions:

- Loss of use and/or limitations on use of NASA IT resources.
- Disciplinary or adverse actions, including dismissal.
- Criminal penalties.
- Employees/contractors being held financially liable for the cost of improper use.

APPENDIX B – QUESTIONS & ANSWERS

1. Is appropriate use of NASA HQ telephones and photocopiers covered under this policy?

Telephone and photocopier usage must be treated differently because of the potential for long-distance and cost per copy charges. The policy for the use of NASA HQ telephones is contained in 2540.1F, Personal Use of Government Office Equipment including IT. The policy for the use of NASA HQ photocopiers is contained in NPR 1490.1G, NASA Printing, Duplicating, and Copying Management. Copies of these regulations may be obtained from the NASA Online Directives Information System (NODIS) at http://nodis3.gsfc.nasa.gov/main_lib.html.

2. Does this policy also pertain to HQ IT resources that have been outsourced, for example the Outsourcing Desktop Initiative for NASA (ODIN) software and equipment?

The policy contained herein applies to any HQ IT resource, whether Government-owned or simply Government provided.

3. May I make personal use of the computer or Internet for extended periods if I do it before or after work hours?

This policy is intended to permit the occasional use of HQ IT resources. It is not intended that HQ employees treat these resources as a substitute for their own equipment or Internet services.

4. May I use E-mail to advertise club meetings, professional associations, community activities, charity events or other worthy causes that are not sponsored by NASA?

While communication with a volunteer charity organization is allowed, the creation and transmission of mass mailings (regardless of subject matter) is not. A maximum number of recipients for a single message are not herein specified. However, reasonable care and judgment must be exercised. The distribution list should generally not exceed more than a few recipients to avoid impacting the throughput and delivery of NASA HQ E-mail systems. For example, sending a personal message to a charitable organization as the single recipient would be acceptable. Sending out a mailing to its entire distribution list of several dozen members would not be acceptable.

5. Can E-mail be used in place of a written document to conduct official NASA business?

E-mail is extremely useful as an informal communication mechanism to facilitate the conduct of NASA business. However, its limitations may prevent it from being used, in all situations, to replace a written document. For instance, E-mail may not be used to commit Government funds or effect a Government contract. In those instances where it is permissible to use E-mail in place of a written document for official NASA business, remember that such electronic mail constitutes an official Agency record subject to NPR 1441.1D - NASA Records Retention

Schedules (w/Change 4, 1/31/08). When in doubt, discuss specific questions with your supervisor.

6. May I install a screen saver on my computer?

You may not install any unauthorized executable programs on your workstation. Only the executable screen saver programs that are installed with your computer may be used. You may set the parameters on these to customize your interface. You may also add pictures to be used in the display via the installed screen savers. However, you must use the same professional discretion in selecting words and images as you would for any item hanging on your wall or otherwise situated in your office environment. In addition to the screen savers, you are also permitted to customize the desktop background (wallpaper) utilizing the computer's standard operating system features. Once again, the caveat for professional discretion applies.

7. May I change the background display on my computer, i.e. constantly display information updates from an outside source? An example of this is a news or stock ticker service.

It is permissible to use your standard browser to display information that is fed to the background display of your desktop from an outside source, provided the Internet service does not require you to install executable software programs on your computer. You must also exercise professional discretion in the subject matter that you choose to display.

8. May I listen to Internet based radio or watch Internet based video using the standard tools that were installed with my computer?

It is permissible to play internet based audio and video provided you utilize the standard software tools installed on your workstation. However, you must be courteous in terms of volume and you must use professional discretion in the frequency and subject matter of the selections you choose to play or view.

9. May I use my computer's CD player to play music?

It is permissible to play music CD's or DVD's on your computer. However, you must be courteous in terms of volume and you must use professional discretion in the subject matter of the selections you choose to play.

10. May I use my personal computer at home to access the Internet via NASA HQ Dial-in service or Virtual Private Network (VPN)?

NASA IT resources and services are primarily for the conduct of official business. They are not a substitute for a private Internet Service Provider (ISP). However, the occasional, limited personal use guidelines apply. Employees must remember that accessing web pages and other Internet facilities leaves a trail that will record that you are originating from a Government access

point. Thus, while on the Internet from a NASA network it will appear that you are representing the Agency.

11. Once I retire can I retain my HQ E-mail account and also my HQ dial-in account to access the Internet?

NASA HQ electronic mail and dial-in accounts are available only for current HQ employees and are not to be used as a substitute for a private ISP. However NASA HQ will forward your E-mail for up to 30 days if a request is made prior to your retirement.

12. I would like to develop a HQ web site for an official NASA project. I know that this web site must be official and in good taste since it will represent NASA. Where can I get information about creating and maintaining a "web site"?

There are a number of important things to consider when developing a NASA home page or placing NASA information on a web site. Any NASA web site is required to be in compliance with section 11.3.9 of NPR 2810.1A, Security of IT, May 16, 2006. A copy of this document may be found at http://nodis-dms.gsfc.nasa.gov/restricted_directives/displayDir.cfm?Internal_ID=N_PR_2810_001A_&page_name=main . Any questions may be addressed to the HQ Webmaster, HQ IT and Communications Division, at 202-358-1767 or E-mailed to webmaster@hq.nasa.gov .

13. Can I send personal instant messages or conduct personal chat sessions on HQ computers or workstations?

NASA HQ recognizes that instant messaging offers a valuable real-time communication channel for collaboration and communication. Currently, HQ has approved and deployed Windows Messenger for PC's and Ichat for Macintosh clients. These products may be used to send brief personal messages, such as checking on children or letting a spouse know you are running late, provided they do not violate the standards of conduct. The installation, Internet access, or use of other instant messaging products from HQ workstations, portable devices, or networks is prohibited.

14. Where can I get more information about HQ IT resources?

If you have questions concerning the use of HQ IT resources, contact your organization's IT Point of Contact (http://www.hq.nasa.gov/itcd/documents/IT_Contacts.xls) or the HQ IT and Communications Division. Additional information can also be obtained at the following web site: <http://www.hq.nasa.gov/itcd>

APPENDIX C - ABBREVIATIONS

CD	Compact Disk
CD-ROM	Compact Disk Read Only Memory
CFR	Code of Federal Regulations
CIO	Chief Information Officer
DVD	Digital Video Disk
E-mail	Electronic Mail
EAR	Export Administration Regulation
Fax	Facsimile
GSA	General Services Administration
HQ	Headquarters
ISP	Internet Service Provider
IT	Information Technology
ITAR	International Traffic in Arms Regulation
NASA	National Aeronautics and Space Administration
NODIS	NASA Online Directives Information System
NPD	NASA Program Directive
NPR	NASA Program Requirement
ODIN	Outsourcing Desktop Initiative for NASA
OMB	Office of Management and Budget
P2P	Peer to Peer
PDA	Personal Digital Assistant
PII	Personally Identifiable Information
SBU	Sensitive but Unclassified
STI	Scientific and Technical Information
VPN	Virtual Private Network