



Department of Defense Education Activity  
**ADMINISTRATIVE INSTRUCTION**

**NUMBER** 6600.01

**Date:** FEB 16 2010

---

---

INFORMATION TECHNOLOGY

**SUBJECT:** Computer Access and Internet Policy

**References:** See Enclosure 1.

1. **PURPOSE.** This Administrative Instruction reissues DoDEA Administrative Instruction 6600.1 (Reference (a)) to update policy and responsibilities for the use and administration of the Department of Defense Education Activity (DoDEA) access to computers and the Internet.

2. **APPLICABILITY.** This Administrative Instruction applies to:

a. The Office of the Director, DoDEA; the Director, Domestic Dependent Elementary and Secondary Schools, and Department of Defense Dependents Schools, Cuba (DDESS/DoDDS-Cuba); the Director, Department of Defense Dependents Schools, Europe (DoDDS-E); the Director, Department of Defense Dependents Schools, Pacific, and Domestic Dependent Elementary and Secondary Schools, Guam (DoDDS-P/DDESS-Guam), (hereafter collectively referred to as "DoDEA Area Directors"); and all DoDEA Area and District Superintendents, School Principals, Teachers, and Support Staff.

b. Volunteers who provide services to DoDEA under the authority of DoD Instruction 1100.21 (Reference (b)).

c. All users of DoDEA Information Technology (IT) resources.

3. **DEFINITIONS.** See Glossary.

4. **POLICY.** It is DoDEA policy that:

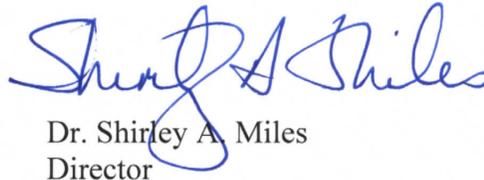
a. The use of DoDEA IT resources shall be permitted for official and authorized purposes including communication, research, and educational or professional development in support of the DoDEA mission.

b. Internet use for educational, administrative, and research purposes will be encouraged and supported in agreement with the terms and conditions contained in the Appendix to Enclosure 3 and/or Appendix to Enclosure 4, while ensuring that government property, including IT resources, is used for authorized purposes only.

c. All use of DoDEA IT resources will be accomplished through individual user accounts, except as specifically authorized by the Designated Approving Authority (DAA).

5. RESPONSIBILITIES. See Enclosure 2.

6. EFFECTIVE DATE. This Administrative Instruction is effective immediately.



Dr. Shirley A. Miles  
Director

Enclosures

1. References
  2. Responsibilities
  3. Appropriate Use Of DoDEA Information Technology Resources  
Terms And Conditions For Employees, Contractors, And Volunteers
  4. Appropriate Use Of DoDEA Information Technology Resources Terms And Conditions  
For DoDEA Students
  5. Wording That Must Be Included in Performance Work Statements and Statements of  
Work
- Glossary

ENCLOSURE 1

REFERENCES

- (a) DoDEA Administrative Instruction 6600.1, "Computer and Internet Access Policy," July 15, 2005 (hereby canceled)
- (b) DoD Instruction 1100.21, "Voluntary Services in the Department of Defense," March 11, 2002, as amended
- (c) Sections 3541 through 3549 of title 44, United States Code
- (d) Office of Management and Budget Circular No. A-130, "Management of Federal Information Resources," November 28, 2000
- (e) DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002, as amended
- (f) DoD Directive 5400.11, "DoD Privacy Program," May 8, 2007
- (g) DoD Chief Information Officer (CIO) Memorandum, "Policy on Use of Department of Defense (DoD) Information Systems— Standard Consent Banner and User Agreement)," May 9, 2008
- (h) DoDEA Regulation 2051.1, "Department of Defense Education Activity Disciplinary Rules and Procedures," April 4, 2008

ENCLOSURE 2

RESPONSIBILITIES

1. DIRECTOR, DODEA; DIRECTOR, DDESS/DODDS-CUBA; DIRECTOR, DODDS E; DIRECTOR, DODDS- P/DDESS-GUAM; DODEA DISTRICT SUPERINTENDENTS, SCHOOL PRINCIPALS. The DoDEA Area Directors, District Superintendents, School Principals, or designees, shall ensure that:

a. A copy of this Administrative Instruction is made available to each DoDEA employee, volunteer, and student under their cognizance who requires a user account.

b. Each DoDEA employee and volunteer requiring a user account signs DoDEA Form 6600.01-F1, "DoDEA Computer and Internet Access Agreement for Employees, Contractors, and Volunteers," (Appendix to Enclosure 3) before being assigned a user account. The signed agreement shall be retained in the local administrative office with a copy furnished to the Area IT Division in accordance with local Area procedures and a copy provided to the employee or volunteer.

c. All employees must comply with initial and annual awareness training as mandated by DoD and in association with sections 3541-3549 of title 44, United States Code (Reference (c)), Office of Management and Budget Circular A-130 (Reference (d)), and DoD Directive 8500.01E (Reference (e)).

d. Each student requiring a user account shall:

(1) Be instructed to read and abide by the terms and conditions contained in DoDEA Form 6600.01-F2, "DoDEA Computer and Internet Access Agreement for Students," (Appendix to Enclosure 4).

(2) Take appropriate precautions to protect DoDEA IT resources including computer equipment, network resources, and data.

(3) Sign DoDEA Form 6600.01-F2 (Appendix to Enclosure 4), together with the student's parent or guardian (if applicable), before he or she is assigned a user account. The signed agreement is to be retained in the administrative office at the student's school for the duration of the student's enrollment. A copy will be provided to the student and, if applicable, the student's parent or guardian.

e. Each Performance Work Statement (PWS) or Statement of Work for contractor services shall specify that all contractors requiring access to DoDEA IT resources will be required to sign DoDEA Form 6600.01-F1 (Appendix to Enclosure 3) as a condition for being assigned a user account with which to access DoDEA IT resources. Enclosure 5 contains language that must be included in the PWS.

f. Each contractor requiring access to DoDEA IT resources, the DoDEA Contracting Officer's Representative (COR) or the DoDEA Program Manager (PM) ensures that the contractor signs DoDEA Form 6600.01 (Appendix to Enclosure 3) before being assigned a user account and thereafter complies with the requirements of completing initial and annual Information Assurance (IA) Awareness training. The signed agreement shall be retained by the COR/PM as a part of the contract with a copy provided to the contractor.

g. Procedures are developed at the local level to implement the DoDEA Computer and Internet Access Policy.

h. DoDEA technical support personnel are not tasked to provide support for problems arising from personal use of DoDEA IT resources.

2. DAA, DODEA. The DAA, DoDEA, or designee, shall ensure that procedures are in place to provide information assurance, including procedures to govern user information assurance training; procedures to make certain that computer user accounts are provided to DoDEA employees, students, contractors, and volunteers only after the appropriate access agreement has been executed; procedures to govern the deletion of user accounts; and procedures to govern retrieving users' files and monitoring their activities using DoDEA IT resources.

3. DODEA FIRST-LINE SUPERVISORS. DoDEA first-line supervisors shall:

a. Request user accounts for all assigned staff (employees and volunteers) requiring access to DoDEA IT resources in accordance with local Area IT Division procedures. The supervisor shall request access privileges required for new and existing users under his or her supervision and ensure that users have the required clearance and a need-to-know for all information to which they are authorized access. The supervisor shall ensure that employees and volunteers needing access to DoDEA IT resources have read and signed DoDEA Form 6600.01-F1 (Appendix to Enclosure 3) before the supervisor requests a user account for the individual. After receiving a new account, the user will have 10 working days to complete the IA Awareness training and 30 working days to complete the privacy training, Protected Personal Information and Personally Identifiable Information (PPI/PII) training.

b. Promptly request termination of access to DoDEA IT resources for employees and volunteers who no longer need their current access to those resources. The supervisor will ensure that needed files are transferred to another user and that the departing user is counseled regarding non-disclosure of sensitive information.

c. Respond promptly to system administrator's periodic requests for review of user privileges.

4. CORS. The CORS shall:

a. Request user accounts for all contractors under their cognizance who require access to DoDEA IT resources. The COR shall request appropriate access and ensure that contractors have the required clearance and a need-to-know for all information to which they will be

authorized access. The COR will ensure that contractors needing access to DoDEA IT resources read and sign DoDEA Form 6600.01-F1 (Appendix to Enclosure 3) before requesting their user accounts. The COR shall also ensure that all contractors complete the IA Awareness training within 10 working days of receiving a new user account and the privacy training, PPI/PII, within 30 working days.

b. Promptly request termination of access to DoDEA IT resources for contractors who no longer need their current access to those resources. The COR will ensure that needed files are transferred to another user and that the departing contractor is counseled regarding non-disclosure of sensitive information.

c. Respond promptly to system administrators' periodic requests for review of user privileges.

5. DODEA EMPLOYEES AND VOLUNTEERS. DoDEA employees and volunteers who require user accounts shall:

a. Read and abide by the terms and conditions contained in Enclosure 3.

b. Sign DoDEA Form 6600.01-F1 (Appendix to Enclosure 3) as a condition, prior to being assigned a user account.

c. Complete initial and annual IA Awareness training within 10 business days of receiving a new user account and the privacy training, PPI/PII, within 30 business days.

d. Take appropriate precautions to protect DoDEA IT resources including computer equipment, network resources, and data.

## ENCLOSURE 3

### APPROPRIATE USE OF DODEA INFORMATION TECHNOLOGY RESOURCES TERMS AND CONDITIONS FOR EMPLOYEES, CONTRACTORS, AND VOLUNTEERS

1. PURPOSE. This attachment defines the appropriate use of DoDEA IT resources. All users of DoDEA information systems must read and agree to abide by these rules before being granted access to DoDEA IT resources.

#### 2. ACCEPTABLE USE

a. DoDEA IT resources, including Internet access and electronic mail systems, are the property of the Federal Government and shall be used for official and authorized purposes only.

(1) Official use includes emergency communications and communication, research or other uses that DoDEA determines are necessary in the interest of the Federal Government.

(2) All authorized government business requiring electronic mail shall be conducted using DoDEA issued electronic mail accounts. Unapproved accounts, such as web-based commercial electronic mail accounts, shall not be used for official government business unless specifically authorized by the DAA. Internet service provider or web-based e-mail systems will be approved only when communication is mission-essential and government owned e-mail systems are not available.

(3) Authorized use of DoDEA IT resources, with respect to employees and volunteers, includes personal communication that is most reasonably made while at the work place (such as brief personal e-mails to check in with family and brief Internet searches), provided that such use:

(a) Does not adversely affect the performance of the employee's official duties and does not adversely impact DoDEA's mission or its operational requirements.

(b) Is of reasonable duration and frequency and, whenever possible, is made during the employee's personal time.

(c) Serves a legitimate public interest, such as enhancing employees' professional skills or allowing employees to remain at their desks rather than requiring lengthy absence from the workplace.

(d) Does not put DoDEA IT resources to uses that would reflect adversely on DoDEA, such as chain letters; unauthorized advertising, soliciting or selling; uses involving gambling or pornography; uses that violate statute or regulation; or other uses that are incompatible with public service.

(e) Involves only limited additional expense to DoDEA and does not overburden DoDEA IT resources, such as may be the case with sending broadcast or group e-mail messages, printing multiple copies of large documents, downloading large or complex graphics files or streaming media.

(f) Utilizes existing IT resources and does not involve unauthorized modification of the existing hardware or software configuration.

(g) Immediately reports all IA related events and potential threats, vulnerabilities, and compromises or suspected compromises involving DoDEA IT resources to the appropriate Information Assurance Officer (IAO).

(h) Protects terminals or workstations from unauthorized access.

(4) Authorized use of IT resources, with respect to contractors, is limited to those uses stated in the Government contract vehicle and those uses authorized by the COR.

(a) DoDEA technical support personnel are expressly prohibited from assisting users with problems arising from their personal use of DoDEA IT resources.

(b) DoDEA is not responsible for the security of personal information communicated using its IT resources and is not responsible for any damages suffered by individuals pursuant to their personal use of DoDEA IT resources.

### 3. UNACCEPTABLE USE

a. DoDEA system users may not install software on DoDEA IT systems except as specifically authorized and approved by the DAA, or designee. This prohibition includes all personally owned software as well as freeware, shareware, patches, or version upgrades.

b. DoDEA system users may not remove or replace any hardware or software provided with their workstation except as specifically approved by the DAA, or designee.

c. DoDEA system users may not connect additional hardware or peripheral devices to DoDEA IT resources except as specifically approved by the DAA, or designee. Additional devices include scanners, printers, modems, and personal digital assistants. The DAA, or designee must approve the installation and use of such equipment and designate the person to perform any installation required.

d. DoDEA specifically prohibits attaching personally owned devices to its IT resources.

e. DoDEA specifically prohibits use of its IT resources to:

(1) Gain or attempt to gain unauthorized access to other systems.

(2) Use as an instrument for theft or knowingly cause the destruction of data belonging to others.

(3) Circumvent, disable, or unilaterally bypass, strain, or test IA mechanisms on any IT resource, IA, or auditing system. This includes disabling virus detection mechanisms or altering the configuration of IT resources.

(4) Pursue private commercial business activities or profit-making ventures, including those conducted on Internet sites.

(5) Endorse any product or service, to participate in lobbying or prohibited partisan political activity, or to engage in any unauthorized fund-raising activity or unauthorized distribution of information related to non-government activities.

(6) Post DoDEA information to external newsgroups, bulletin boards, or other public forums without authorization.

(7) Access known "hacker" sites or download hacking tools without authorization.

(8) Create or knowingly transmit an executable virus program or any virus infected files.

(9) Create or knowingly access, download, view, store, copy, or transmit sexually explicit or sexually oriented materials; including Uniform Resource Locator, links to any pornographic web sites.

(10) Create or knowingly access, download, view, store, copy, or transmit materials related to gambling, illegal weapons, terrorist activities or any other illegal or prohibited activities.

(11) Create or knowingly access, download, view, store, copy, or transmit material or communication that is illegal or offensive to others, such as hate speech and any material that ridicules others based on race, creed, religion, color, sex, disability, national origin or sexual orientation.

(12) Create or knowingly forward, transmit, or copy chain letters regardless of the subject matter.

(13) Knowingly acquire, use, reproduce, transmit, or distribute any controlled information, except as authorized (e.g., fair use). Controlled information may include music, video, graphic files, data or computer software protected by privacy laws, copyright, trademark, or other intellectual property rights.

#### 4. IA

(a) In accordance with Reference (e), user accounts that provide access to DoDEA information resources must be established, maintained, and used in such way as to protect those resources. Each user is responsible for any activity conducted using his or her account. An individual user may only use that account to which he or she is assigned and may not allow others to use his or her account. The user's password must, at all times, be known only to the user. The user may not share his or her password with anyone, including the supervisor. Users are responsible for taking reasonable precautions to maintain the security of their accounts and the data to which they are authorized access.

(b) DoDEA information systems contain valuable and sensitive government information, and many DoDEA systems are connected to other DoD systems. Each user must exercise care to protect against actions that could introduce system-wide vulnerabilities.

(c) The system user will only use the computer account(s) specifically issued to him or her and will use the account(s) for official and/or authorized purposes only.

(d) System users will not use their accounts to access data to which they have not been given specific authorization, even if the account allows such access.

(e) System users will report any suspicious activity or suspected IA-related event to their local technical support personnel or IAO. In the event that the user notifies only the supervisor, then the supervisor must ensure that technical support personnel or IAO is notified.

(f) Classified material should not be stored on DoDEA IT resources other than those specifically designated and approved for that purpose. Users of these designated resources will ensure that system media and output are properly marked, controlled, stored, transported, and destroyed based on the classification or sensitivity and need-to-know.

5. WEB PUBLISHING. In accordance with DoD Directive 5400.11 (Reference (f)), users who are responsible for publishing content to DoDEA Public web pages will not publish or disclose any personal identifiable information except as authorized by the Chief, Office of Communications, DoDEA. Users agree to follow the DoDEA Web Publishing Guidelines, which can be found in the Publications section accessible via the DoDEA home page at [www.dodea.edu](http://www.dodea.edu). In particular, users will not publish private personal information such as the name, social security number, photograph, home address, e-mail address, or telephone number of any individual except as specifically permitted by the DoDEA Web Publishing Guidelines.

#### Appendix:

DoDEA Computer and Internet Access Agreement for Employees, Contractors, and Volunteers

**DoDEA COMPUTER AND INTERNET ACCESS AGREEMENT  
FOR EMPLOYEES, CONTRACTORS, AND VOLUNTEERS**

**DoD STANDARD MANDATORY NOTICE AND CONSENT PROVISION  
FOR ALL DoD INFORMATION SYSTEM USER AGREEMENTS**

By signing this agreement, you acknowledge and consent that when you access DoDEA information systems:

a. You are accessing a U.S. Government information system (which includes any device attached to this information system) that is provided for U.S. Government authorized use only.

b. You consent to the following conditions:

(1) The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security monitoring, network operations and defense, personnel misconduct, law enforcement, and counterintelligence investigations.

(2) At any time, the U.S. Government may inspect and seize data stored on this information system.

(3) Communications using, or data stored on, this information system are not private, and are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.

(4) This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests, not for personal benefit or privacy.

(5) Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:

(a) Nothing in this User Agreement shall be interpreted to limit the user's consent, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.

(b) The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose, including personnel misconduct, law enforcement, or counterintelligence investigation. However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.

**DoDEA COMPUTER AND INTERNET ACCESS AGREEMENT  
FOR EMPLOYEES, CONTRACTORS, AND VOLUNTEERS****DoD STANDARD MANDATORY NOTICE AND CONSENT PROVISION  
FOR ALL DoD INFORMATION SYSTEM USER AGREEMENTS** *(Continued)*

(c) Protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.

(d) Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.

(e) A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.

(f) These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

(6) In cases where the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching (i.e., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.

(7) All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner according to the Chief Information Officer Memorandum (Reference (h)), (hereafter referred to as a "banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

**DoDEA COMPUTER AND INTERNET ACCESS AGREEMENT  
FOR EMPLOYEES, CONTRACTORS, AND VOLUNTEERS**

**PRIVACY ACT STATEMENT**

**AUTHORITY:** 10 U.S.C. 2164 and 20 U.S.C. 921-932, authorizing DoD Directive 1342.20, "DoD Education Activity" (2007), authorizing DoD Education Activity Administrative Instruction 6600.1 (2010).

**PRINCIPAL PURPOSE(S):** The information on this form is used to authorize an individual to use government-owned computer resources in accordance with, and subject to enforcement provisions of, DoD and DoDEA policies governing computer and Internet usage.

**ROUTINE USE(S):** Disclosure of germane information contained in this form within the Department of Defense is authorized upon a demonstrated "need to know" to perform an official duty. Routine disclosure of relevant and necessary information is authorized to agencies outside of the DoD by DoD Privacy Act Systems Notices, which may be found at <http://www.defenselink.mil/privacy/notices/osd/>. Records are maintained in the workplace.

**DISCLOSURE:** Voluntary; however, no individual is permitted to use DoDEA-controlled computer resources until they have signed this statement indicating agreement to use such equipment only in accordance with the DoDEA Appropriate Use of DoDEA Information Technology Resources - Terms and Conditions for Employees, Contractors, and Volunteers.

**1. INDIVIDUAL INFORMATION** *(please print or type)*

a. NAME <i>(Last, first, middle initial)</i>	b. TELEPHONE NUMBER <i>(Include area code)</i>
c. SCHOOL/OFFICE/DIVISION/BRANCH	d. SUPERVISOR <i>(Print and Sign)</i>

**2. AGREEMENT**

I, *(print name)* \_\_\_\_\_, am aware of the contents of DoDEA Administrative Instruction 6600.1, which can be found in the Regulations section accessible via the DoDEA home page at [www.dodea.edu](http://www.dodea.edu), and includes the Appropriate Use of DoDEA Information Technology Resources. I have read these documents. In consideration for being given a user account and access to DoDEA Information Technology (IT) resources, I hereby agree to abide by the terms and conditions as stated.

I understand that I have no expectation of privacy when using DoDEA IT resources and that all individuals using DoDEA IT resources are subject to having their activities on the system monitored and recorded. I expressly consent to such monitoring. I am aware that, if such monitoring reveals possible evidence of criminal activity or activity in violation of the Appropriate Use of DoDEA Information Technology Resources - Terms and Conditions for Employees, Contractors, and Volunteers (Enclosure 3), the evidence of such activity may be provided to law enforcement officials and/or to DoDEA officials for use in possible adverse personnel actions or criminal proceedings. I understand that all files stored on DoDEA IT resources are the property of DoDEA and can be made available to DoDEA employees as necessary.

I understand that if I violate the terms and conditions contained in the Appropriate Use of DoDEA Information Technology Resources - Terms and Conditions for Employees, Contractors, and Volunteers (Enclosure 3), such violation(s) may result in the suspension of my computer account or restriction of network privileges and, if warranted, disciplinary or legal action may be taken against me.

a. SIGNATURE	b. DATE (YYYYMMDD)
--------------	--------------------

## ENCLOSURE 4

### APPROPRIATE USE OF DODEA INFORMATION TECHNOLOGY RESOURCES TERMS AND CONDITIONS FOR DODEA STUDENTS

#### 1. USE OF INFORMATION TECHNOLOGY RESOURCES

a. Students will use DoDEA's IT resources, including computers, electronic mail, and internet access, only in support of education and for research consistent with the educational objectives of DoDEA.

b. Students will respect and adhere to all of the rules governing access to, and use of, DoDEA's IT resources.

c. Students will be polite in all electronic communication. Students will use courteous and respectful language and/or images in their messages to others. Students will not swear, use vulgarities, or use harsh, abusive, sexual, or disrespectful language and/or images.

d. Students will not use DoDEA's IT resources to:

(1) Deliberately disrupt network use by others. Therefore, students will not send "chain letters" or "broadcast" messages to individuals or to lists of individuals.

(2) Gain, or attempt to gain, unauthorized access to other computer systems.

(3) Attempt to harm or destroy data of another user, the internet, or any other network. This includes creating or knowingly transmitting a computer virus or worm, or attempting unauthorized access to files, computers, or networks (i.e., "hacking").

(4) Attempt to disable any IT security or auditing system.

(5) Pursue private commercial business activities, including those conducted on Internet sites (online buying and selling sites).

(6) Create, access, download, view, store, copy, send, or knowingly receive material that is illegal or offensive to others, such as hate speech or any material that ridicules others based on race, creed, religion, color, sex disability, national origin, or sexual orientation.

(7) Create, access, download, view, store, copy, send, or knowingly receive material that is obscene, pornographic, or sexually suggestive.

(8) Participate in illegal or prohibited activities, such as those related to gambling, illegal weapons, or terrorist activities.

## 2. SECURITY OF DODEA IT RESOURCES

- a. Security on any computer system is a high priority. Students will notify a teacher if they notice a security problem.
- b. Students will only use the computer accounts issued to them and will log off the system promptly when finished. Actions performed using a student's account will be considered to have been done by that student. It is the student's responsibility to protect his or her account and password. Students will not give their user passwords to other individuals.

## 3. PRIVILEGE OF USING IT RESOURCES

- a. The use of the network is a privilege, not a right. A use that is inconsistent with these Terms and Conditions may result in the termination of student privileges.
- b. Electronic transmissions, including electronic mail, are not private. Individual communications and system access will be monitored.
- c. Students who misuse DoDEA IT resources are subject to disciplinary measures such as those prescribed in DoDEA Regulation 2051.1 (Reference (h)). At the discretion of the principal, the student may lose the privilege of using DoDEA IT resources permanently and may be suspended or expelled from school.

4. DOD POLICY ON USE. By signing DoDEA Form 6600.01-F2 (Appendix to Enclosure 4), you acknowledge and consent that when you access DoDEA information systems:

- a. You are accessing a U.S. Government information system (which includes any device attached to this information system) that is provided for U.S. Government authorized use only.
- b. You consent to the following conditions:

(1) The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security monitoring, network operations and defense, personnel misconduct, law enforcement, and counterintelligence investigations.

(2) At any time, the U.S. Government may inspect and seize data stored on this information system.

(3) Communications using, or data stored on, this information system are not private, and are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.

(4) This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests, not for personal benefit or privacy.

(5) Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:

(a) Nothing in this User Agreement shall be interpreted to limit the user's consent, or in any other way restrict or affect any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.

(b) The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.

(c) Protection of a privilege, or a duty of confidentiality is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.

(d) Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.

(e) A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.

(f) These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

(6) In cases where the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (i.e., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.

(7) All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner, in accordance with Reference (g), ( hereafter referred to as a "banner"). When a banner is used, the banner functions to remind the user of the condition that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

(8) Students, if under the age of 18, must also have their parent or guardian sign DoDEA Form 6600.01-F2. By signing this agreement, the student and parent or guardian agree to follow the rules set forth in DoDEA Form 6600.01-F2 and to report any misuse of the computer network or the Internet to a teacher.

5. OTHER. If students have any questions about appropriate computer use, they will ask their teacher.

Appendix:

DoDEA Computer and Internet Access Agreement for Students

**DoDEA COMPUTER AND INTERNET ACCESS AGREEMENT FOR STUDENTS****DoD STANDARD MANDATORY NOTICE AND CONSENT PROVISION  
FOR ALL DoD INFORMATION SYSTEM USER AGREEMENTS**

By signing this agreement, you acknowledge and consent that when you access DoDEA information systems:

a. You are accessing a U.S. Government information system (which includes any device attached to this information system) that is provided for U.S. Government authorized use only.

b. You consent to the following conditions:

(1) The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security monitoring, network operations and defense, personnel misconduct, law enforcement, and counterintelligence investigations.

(2) At any time, the U.S. Government may inspect and seize data stored on this information system.

(3) Communications using, or data stored on, this information system are not private, and are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.

(4) This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests, not for personal benefit or privacy.

(5) Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:

(a) Nothing in this User Agreement shall be interpreted to limit the user's consent, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.

(b) The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose, including personnel misconduct, law enforcement, or counterintelligence investigation. However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.

**DoDEA COMPUTER AND INTERNET ACCESS AGREEMENT FOR STUDENTS****DoD STANDARD MANDATORY NOTICE AND CONSENT PROVISION  
FOR ALL DoD INFORMATION SYSTEM USER AGREEMENTS** *(Continued)*

(c) Protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.

(d) Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.

(e) A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.

(f) These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

(6) In cases where the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching (i.e., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.

(7) All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner according to the Chief Information Officer Memorandum (Reference (h)), (hereafter referred to as a "banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

**DoDEA COMPUTER AND INTERNET ACCESS AGREEMENT FOR STUDENTS**

**PRIVACY ACT STATEMENT**

**AUTHORITY:** 10 U.S.C. 2164 and 20 U.S.C. 921-932, authorizing DoD Directive 1342.20, "DoD Education Activity" (2007), authorizing DoD Education Activity Administrative Instruction 6600.1 (2010).

**PRINCIPAL PURPOSE(S):** The information on this form is used to authorize an individual student to use government-owned computer resources in accordance with, and subject to enforcement provisions of, DoD and DoDEA policies governing computer and Internet usage.

**ROUTINE USE(S):** Disclosure of germane information contained in this form within the Department of Defense is authorized upon a demonstrated "need to know" to perform an official duty. Routine disclosure of relevant and necessary information is authorized to agencies outside of the DoD by DoD Privacy Act Systems Notices, which may be found at <http://www.defenselink.mil/privacy/notices/osd/>. Records are maintained at the school level in student records for the duration of the student's enrollment.

**DISCLOSURE:** Voluntary; however, no individual is permitted to use DoDEA-controlled computer resources until they have signed this statement indicating agreement to use such equipment only in accordance with the DoDEA Appropriate Use of DoDEA Information Technology Resources - Terms and Conditions for DoDEA Students.

**1. STUDENT INFORMATION** *(Please print or type)*

a. NAME <i>(Last, first, middle initial)</i>	b. PARENT/GUARDIAN NAME <i>(Print)</i>
c. SCHOOL	d. TEACHER NAME/GRADE/SIGNATURE

**2. STUDENT AGREEMENT**

I, *(print name)* \_\_\_\_\_, have received instruction in the appropriate use of DoDEA information technology resources, and I agree to abide by them. If I violate the Terms and Conditions, I understand that I may lose all access privileges on the DoDEA network, and, furthermore, may be subject to school disciplinary and/or appropriate legal actions.

a. STUDENT SIGNATURE	b. DATE <i>(YYYYMMDD)</i>
----------------------	---------------------------

**3. PARENT OR GUARDIAN** *(If student is under the age of 18, a parent or guardian must also read and sign this agreement.)*

I, *(print name)* \_\_\_\_\_, have read the Appropriate Use of DoDEA Information Technology Resources - Terms and Conditions for DoDEA Students (attachment 1). I understand that my child must abide by these Terms and Conditions. I understand that if my child violates these standards, he/she may lose all access privileges on the DoDEA network and may be subject to school disciplinary and/or appropriate legal actions. I understand that computer and network access is being provided for educational purposes.

a. PARENT OR GUARDIAN SIGNATURE	b. DATE <i>(YYYYMMDD)</i>
---------------------------------	---------------------------

ENCLOSURE 5

WORDING THAT MUST BE INCLUDED IN PERFORMANCE WORK STATEMENTS  
AND STATEMENTS OF WORK

The following paragraph shall be included in the “Description of Services” section of all Performance Work Statements and Statements of Work:

Computer and Internet Access Agreement: Contractor employees are required to sign DoDEA Form 6600.01-F1, “DoDEA Computer and Internet Access Agreement for Employees, Contractors, And Volunteers,” (Appendix to Enclosure 3), prior to gaining access to DoDEA’s information technology resources. This includes connecting to a DoDEA network in order to obtain access to the Internet. No user’s account will be assigned to a contractor unless Form 6600.01-F1, “DoDEA Computer and Internet Access Agreement for Employees, Contractors, And Volunteers,” (Appendix to Enclosure 3), has been signed and is on file. A record of the signed agreement shall be maintained by the contractor and a copy shall be provided to the DoDEA contracting officer’s representative.

## GLOSSARY

### PART I. ABBREVIATIONS AND ACRONYMS

CIO	Chief Information Officer
COR	Contracting Officer's Representative
DAA	Designated Approving Authority
IA	Information Assurance
IAO	Information Assurance Officer
IT	Information Technology
PM	Program Manager
PWS	Performance Work Statement
PPI/PII	Protected Personal Information and Personally Identifiable Information

### PART II. DEFINITIONS

User account. The DoDEA user account provides login access to DoDEA Information Technology Resources, including access to the Internet and/or DoDEA's electronic mail system.

IT resources. The hardware, firmware, and software used as part of the information system to perform DoDEA information functions. This includes computing devices, peripherals, telecommunications, automated information systems, and automatic data processing equipment. IT resources include any set of information resources, such as any assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, display, process, store, transmit, use, and/or control data or information. This includes automated information system applications, enclaves, outsourced IT-based processes, and platform IT interconnections.

DAA. IT official with the authority to formally assume the responsibility for operating a system or network at an acceptable level of risk. The DAA for DoDEA is the DoDEA CIO. The Area IT Chiefs are responsible for enforcing policies set forth by the DoDEA CIO.

IA. Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.