**DEPARTMENT OF DEFENSE**
**EDUCATION ACTIVITY**
4040 NORTH FAIRFAX DRIVE
ARLINGTON, VIRGINIA 22203-1635

Information Technology

DoDEA Administrative Instruction 6600.1
July 15, 2005

DEPARTMENT OF DEFENSE EDUCATION ACTIVITY
ADMINISTRATIVE INSTRUCTION

SUBJECT: Computer and Internet Access Policy

References: (a) DoDEA Administrative Instruction 6600.1 "Computer Access and Internet Policy," August 29, 1997 (hereby canceled)
(b) DoD Instruction 1100.21, "Voluntary Services in the Department of Defense," March 11, 2002
(c) Department of Defense Education Activity Memorandum, "Appointment of Department of Defense Education Activity (DoDEA) Designated Approving Authority and Certification Authority," September 16, 2004
(d) DoD Regulation 5500.7-R, "Joint Ethics Regulation," August 30, 1993, as amended
(e) Chairman of the Joint Chiefs of Staff Manual 6510.01 "Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND)," March 25, 2003
(f) DoD Directive 5400.11, "DoD Privacy Program," December 13, 1999

## 1. REISSUANCE AND PURPOSE

This Administrative Instruction reissues 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 AND SCOPE

This Administrative Instruction applies to:

2.1. The Office of the Director, Department of Defense Education Activity; 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); and all DoDEA District Superintendents, School Principals, Teachers, and Support Staff.

2.2. Volunteers who provide services to DoDEA under the authority of reference (b).

2.3. All use of DoDEA information technology (IT) resources.

## 3. DEFINITIONS

3.1. 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.

3.2. Information Technology 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 assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.

3.3. Designated Approving Authority (DAA). IT official with the authority to formally assume the responsibility for operating a system or network at an acceptable level of risk. In accordance with reference (c), the DAA for DoDEA is the DoDEA Chief Information Officer (CIO). The Area IT Chiefs serve as DAAs for their respective areas and are responsible for enforcing policies set forth by the DoDEA CIO.

## 4. POLICY

It is DoDEA policy that:

4.1. In accordance with reference (d), 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.

4.2. Internet use for educational, administrative, and research purposes will be encouraged and supported in accordance with the terms and conditions contained in enclosure 1, attachment 1, while ensuring that government property, including IT resources, is used for authorized purposes only.

4.3. All use of DoDEA IT resources will be accomplished through user accounts, except as specifically authorized by the DAA.

## 5. RESPONSIBILITIES

5.1. The Director, Domestic Dependent Elementary and Secondary Schools and Cuba; the Director, Department of Defense Dependents Schools, Europe; the Director, Department of Defense Dependents Schools, Pacific and Domestic Dependent Elementary and Secondary

Schools, Guam; and all DoDEA District Superintendents, School Principals, or designees, shall ensure that:

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

5.1.2. Each DoDEA employee and volunteer requiring a user account signs DoDEA Form 6600.1-F1 (enclosure 1) before being assigned a user account. The signed agreement is to be retained in the local administrative office with a copy provided to the employee or volunteer.

5.1.3. Each student requiring a user account:

5.1.3.1. Is instructed to read and abide by the terms and conditions contained in enclosure 2, attachment 1.

5.1.3.2. Takes appropriate precautions to protect DoDEA IT resources including computer equipment, network resources, and data.

5.1.3.3. Together with the student's parent or guardian, if applicable, signs DoDEA Form 6600.1-F2 (enclosure 2) before the student 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.

5.1.4. Each Performance Work Statement (PWS) for contractor services specifies that all contractors requiring access to DoDEA IT resources will be required to sign DoDEA Form 6600.1-F1 as a condition for being assigned a user account with which to access DoDEA IT resources. Enclosure 3 contains wording to be included in the PWS.

5.1.5. For each contractor requiring access to DoDEA IT resources, the Contracting Officer's Representative (COR) or Program Manager (PM) ensures that the contractor signs DoDEA Form 6600.1-F1 before being assigned a user account. The signed agreement is to be retained by the COR/PM as a part of the contract with a copy provided to the contractor.

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

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

5.2. The Designated Approving Authority, 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.

5.3. DoDEA First-Line Supervisors shall:

5.3.1. Request user accounts for all assigned staff (employees and volunteers) requiring access to DoDEA IT resources. The supervisor will determine 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 will ensure that employees and volunteers needing access to DoDEA IT resources have read and signed DoDEA Form 6600.1-F1 before requesting their user accounts.

5.3.2. 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.

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

5.4. DoDEA Contracting Officers' Representatives (CORs) shall:

5.4.1. Request user accounts for all contractors under their cognizance who require access to DoDEA IT resources. The COR will determine 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 6600.1-F1 before requesting their user accounts.

5.4.2. 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.

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

5.5. DoDEA Employees and Volunteers who require user accounts shall:

5.5.1. Read and abide by the terms and conditions contained in enclosure 1, attachment 1.

5.5.2. Sign DoDEA Form 6600.1-F1 as a condition precedent to being assigned a user account.

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

6. EFFECTIVE DATE AND IMPLEMENTATION

This Administrative Instruction is effective immediately.

Joseph D. Tafoya
Director

Enclosures - 3

E1. DoDEA Form 6600.1-F1, "DoDEA Computer and Internet Access Agreement for Employees, Contractors, and Volunteers"

E2. DoDEA Form 6600.1-F2, "DoDEA Computer and Internet Access Agreement for Students"

E3. Wording to Be Included in Performance Work Statements

# E1. ENCLOSURE 1
# DODEA FORM 6600.1-F1

**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" (1992), authorizing DoD Education Activity Administrative Instruction 6600.1 (2004).
**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 *(Last, first, middle initial)* | b. TELEPHONE NUMBER *(Include area code)* |
|---|---|
| | |

| c. SCHOOL/OFFICE/DIVISION/BRANCH | d. SUPERVISOR |
|---|---|
| | |

**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, and includes the Appropriate Use of DoDEA Information Technology Resources - Terms and Conditions for Employees, Contractors, and Volunteers (attachment 1). 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 (attachment 1), 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 (attachment 1), 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)* |
|---|---|
| | |

**DoDEA FORM 6600.1-F1, JUN 2004**

Reset

Attachment – 1
E1.A1. Appropriate Use of DoDEA Information Technology Resources Terms and Conditions for Employees, Contractors, and Volunteers

# E1.A1. ENCLOSURE 1 (ATTACHMENT 1)

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

### E1.A1.1. PURPOSE

This attachment defines the appropriate use of Department of Defense Education Activity (DoDEA) information technology (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.

### E1.A1.2. ACCEPTABLE USE

E1.A1.2.1. DoDEA IT resources, including Internet access and electronic mail systems, are the property of the Federal Government and, in accordance with reference (d), shall be used for official and authorized purposes only.

E1.A1.2.1.1. Official use includes emergency communications and communication, research or other uses that DoDEA determines are necessary in the interest of the Federal Government.

E1.A1.2.1.2. In accordance with reference (e), all authorized government business requiring electronic mail shall be conducted using DoDEA issued electronic mail accounts. Unapproved accounts, such as AOL, Hotmail, or Yahoo, will not be used for official government business unless specifically authorized to do so by the DAA. Internet service provider (ISP) or web-based e-mail systems will be approved only when communication is mission-essential and government owned e-mail systems are not available.

E1.A1.2.1.3. Authorized use of DoDEA IT resources, with respect to employees and volunteers, includes personal communications that are 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:

E1.A1.2.1.3.1. Does not adversely affect the performance of the employee's official duties and does not adversely impact DoDEA's mission or its operational requirements.

E1.A1.2.1.3.2. Is of reasonable duration and frequency and, whenever possible, is made during the employee's personal time.

E1.A1.2.1.3.3. 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.

E1.A1.2.1.3.4. 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 pornography; uses that violate statute or regulation; or other uses that are incompatible with public service.

E1.A1.2.1.3.5. 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, or downloading large or complex graphics files or streaming media.

E1.A1.2.1.3.6. Is of existing IT resources and does not involve unauthorized modification of the existing hardware or software configuration.

E1.A1.2.1.4. 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 Contracting Officer's Representative (COR).

E1.A1.2.2. DoDEA technical support personnel are expressly prohibited from assisting users with problems arising from their personal use of DoDEA IT resources.

E1.A1.2.3. 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.

E1.A1.3. UNACCEPTABLE USE

E1.A1.3.1. DoDEA system users may not install software on DoDEA IT systems except as specifically authorized by DoDEA Administrative Instruction 6700.6, "Acquisition, Use, Management, and Development of Software," February 19, 2002, and approved by the DAA or designee. This prohibition includes all personally owned software as well as freeware, shareware, patches, or version upgrades.

E1.A1.3.2. 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.

E1.A1.3.3. 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 (PDAs). The DAA or designee must approve the installation and use of such equipment and designate the person to perform any installation required.

E1.A1.3.4. DoDEA specifically prohibits attaching personally owned devices to its IT resources.

E1.A1.3.5. DoDEA specifically prohibits use of its IT resources for any of the following:

E1.A1.3.5.1. To gain or attempt to gain unauthorized access to other systems.

E1.A1.3.5.2. To use as an instrument for theft or knowingly cause the destruction of data belonging to others.

E1.A1.3.5.3. To circumvent or disable any IT resource or Internet security or auditing system. This includes disabling virus detection mechanisms or altering the configuration of IT resources.

E1.A1.3.5.4. To pursue private commercial business activities or profit-making ventures, including those conducted on Internet sites.

E1.A1.3.5.5. To 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.

E1.A1.3.5.6. To post DoDEA information to external newsgroups, bulletin boards, or other public forums without authorization.

E1.A1.3.5.7. To access known "hacker" sites or download hacking tools without authorization.

E1.A1.3.5.8. To create or knowingly transmit an executable virus program or any virus infected files.

E1.A1.3.5.9. To create or knowingly access, download, view, store, copy, or transmit sexually explicit or sexually oriented materials, including Uniform Resource Locator (URL) links to any pornographic web sites.

E1.A1.3.5.10. To 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.

E1.A1.3.5.11. To 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.

E1.A1.3.5.12. To create or knowingly forward, transmit, or copy chain letters, regardless of the subject matter.

E1.A1.3.5.13. To 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.

E1.A1.4. INFORMATION ASSURANCE (IA)

E1.A1.4.1. 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.

E1.A1.4.2. DoDEA information systems contain valuable and sometimes sensitive government information, and many DoDEA systems are connected to other Department of Defense (DoD) systems. Each user must exercise care to protect against actions that could introduce system-wide vulnerabilities.

E1.A1.4.3. 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.

E1.A1.4.4. System users will not use their accounts to knowingly access data to which they have not been given specific authorization, even if the account allows such access.

E1.A1.4.5. System users will report any suspicious activity or suspected IA-related event to local technical support personnel or to their supervisor. In the event that the user notifies only the supervisor, then the supervisor must ensure that technical support personnel are notified.

E1.A1.4.6. Classified material should not be stored on DoDEA IT resources other than those specifically designated and approved for that purpose.

E1.A1.5. WEB PUBLISHING

In accordance with reference (f), users who are responsible for publishing content to DoDEA web pages will not publish or disclose any personal information except as authorized. 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. In particular, users will not publish private 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.

# E2. ENCLOSURE 2
# DODEA FORM 6600.1-F2

**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" (1992), authorizing DoD Education Activity Administrative Instruction 6600.1 (2004).
**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 *(Last, first, middle initial)* | b. PARENT/GUARDIAN |
|---|---|
| c. SCHOOL | d. TEACHER/GRADE |

**2. STUDENT AGREEMENT**

I, *(print name)* _____, have received instruction in the appropriate use of DoDEA information technology resources; I have read and understood the Appropriate Use of DoDEA Information Technology Resources - Terms and Conditions for DoDEA Students (attachment 1) 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 *(YYYYMMDD)* |
|---|---|

**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 *(YYYYMMDD)* |
|---|---|

**DoDEA FORM 6600.1-F2, JUN 2004**

Reset

Attachment – 1
E2.A1. Appropriate Use of DoDEA Information Technology Resources Terms and Conditions for DoDEA Students

## E2.A1. ENCLOSURE 2 (ATTACHMENT1)

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

### E2.A1.1. USE OF INFORMATION TECHNOLOGY RESOURCES

E2.A1.1.1. 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.

E2.A1.1.2. Students will respect and adhere to all of the rules governing access to and use of DoDEA's IT resources.

E2.A1.1.3. Students will be polite in all electronic communication. Students will use courteous and respectful language in their messages to others. Students will not swear, use vulgarities, or use harsh, abusive, sexual, or disrespectful language.

E2.A1.1.4. Students will not use DoDEA's IT resources:

E2.A1.1.4.1. To deliberately disrupt network use by others. Therefore, students will not send "chain letters" or "broadcast" messages to individuals or to lists of individuals.

E2.A1.1.4.2. To gain or attempt to gain unauthorized access to other computer systems.

E2.A1.1.4.3. To 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").

E2.A1.1.4.4. To attempt to disable any IT security or auditing system.

E2.A1.1.4.5. To pursue private commercial business activities, including those conducted on Internet sites such as eBay.

E2.A1.1.4.6. To 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.

E2.A1.1.4.7. To create, access, download, view, store, copy, send, or knowingly receive material that is obscene, pornographic, or sexually suggestive.

E2.A1.1.4.8. To participate in illegal or prohibited activities, such as those related to gambling, illegal weapons, or terrorist activities.

E2.A1.2. SECURITY OF DODEA IT RESOURCES

E2.A1.2.1. Security on any computer system is a high priority. Students will notify a teacher if they notice a security problem.

E2.A1.2.2. 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 their account and password. Students will not give their user passwords to other individuals.

E2.A1.3. PRIVILEGE OF USING IT RESOURCES

E2.A1.3.1. The use of the network is a privilege, not a right, and use which is inconsistent with these Terms and Conditions may result in the cancellation of student privileges.

E2.A1.3.2. Electronic transmissions, including electronic mail, are not private and individual communications and system access will be monitored.

E2.A1.3.3. Students who misuse DoDEA IT resources are subject to disciplinary measures such as those prescribed in DoDEA Regulation 2051.1, "Department of Defense Education Activity Disciplinary Rules and Procedures," August 16, 1996. 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.

E2.A1.4. OTHER

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

## E3. ENCLOSURE 3

## WORDING TO BE INCLUDED IN PERFORMANCE WORK STATEMENTS

The following paragraph shall be included in the "Description of Services" section of all Performance Work Statements.

Computer and Internet Access Agreement: Contractor employees are required to sign DoDEA Form 6600.1-F1, "DoDEA Computer and Internet Access Agreement for Employees, Contractors, and Volunteers," June 2004, 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 DoDEA Form 6600.1-F1 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 Contracting Officer's Representative (COR).