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.