CESA #9 TECHNOLOGY/INTERNET/ELECTRONIC MAIL USAGE POLICY AND CHILD INTERNET PROTECTION ACT – INTERNET SAFETY POLICY

CESA #9 provides its employees with technology, including computer software, scanners, printers, fax machines, e-mail, Internet, telephone, voice mail and other methods of electronic communication. This technology has the limited purpose of supporting the mission of CESA #9.

The Agency encourages its employees to use this technology to communicate with others and to access the wide-range of information both within Agency resources and external resources. Employees are further encouraged to enhance their productivity and upgrade their work skills through appropriate use of the network. The network will also assist them in communicating with school districts, school administrators, parents, teachers, peers and other agencies as may be required by the duties of their position with CESA #9. CESA #9 expects all employees to use the technology systems in a responsible manner. CESA #9 reserves the right to restrict or revoke any employee's authorization for use of and access to these systems at any time, for any reason.

Appropriate Usage

CESA #9 technology, as well as its electronic communication systems and equipment, are provided for the purpose of conducting the business of CESA #9. Employees may use this equipment for the purposes relating to CESA #9 business and to carry out the duties of their employment at CESA #9. Personal use of CESA #9 electronic communication equipment and technology should be limited to the reasonable use that does not violate this policy, interfere with the employee's performance of his or her duties, interfere with or offend other employees or disrupt the operation of CESA #9. Employees will use the technology for purposes related to the Agency's mission and will not attempt to extend their use beyond their authorized limits of access nor attempt to disrupt the network's performance or destroy data. Each employee may have at least one account and password assigned. The employee is responsible for the use of each assigned account, and shall take reasonable precautions to prevent others from using them.

No Expectation of Privacy

CESA #9 electronic equipment, communication system and technology are solely the property of CESA #9. All electronic communications transmitted by, received from, or stored in or on CESA #9 electronic equipment, communications system or computer resources are owned by CESA #9. Employees have no expectation of privacy with regard to the utilization of the equipment, or the information, messages, files and any other data contained thereon. CESA #9 may access, search, monitor, and/or disclose any communications at any time without prior notice being given. Additionally, all e-mail/voice mail messages are the property of CESA #9. Nothing residing in an employee's computer

equipment system, or files, CESA #9 e-mail system, the employee's voice mailbox or other equipment will be deemed personal, private or confidential. Data or information residing in or on such equipment may be subject to the Wisconsin Public Records law depending upon the nature of the information. Additionally, one must be mindful that such information may be discoverable in legal actions.

CESA #9 employees will use reasonable efforts to maintain the accuracy and usability of data and to maintain the operating condition of Agency computer equipment and software. Employees will report immediately any suspected or known problems with regard to the technology equipment to the technology department.

Prohibited Uses

The following uses of CESA #9 electronic communication system are strictly prohibited:

Use of e-mail, voice mail, or other aspect of CESA #9 electronic communication system in a manner that could be disruptive, offensive or harmful to the morale of other CESA #9 employees, vendors, contractors, customers or other third parties.

Downloading, displays, viewing, accessing, retrieving, storage and/or transmission of sexually offensive text or images or otherwise offensive images, documents, cartoons, messages, ethnic slurs, racial epithets, or anything that may be construed as threatening, harassing or intimidating to others based on their gender, race, national origin, age, disability, religion, sexual orientation or any other basis protected by applicable law.

Excessive use of CESA #9 electronic communication systems for personal recreation, including but not limited to playing games, internet browsing, on-line shopping or trading, or conducting a personal business unrelated to the business of CESA #9.

Use of the Agency's electronic communication systems for commercial purposes not related to Agency business.

Solicitation of other employees, customers, vendors or other third parties for commercial purposes, lobbying, political causes, sending pornographic or harassing materials, participation in illegal activities, outside organizations, unrelated to the business of CESA #9, or other non-job related purposes.

Illegal activities, including but not limited to gambling or trafficking in pornography.

Unauthorized accessing or attempting to access, or transmittal of confidential CESA #9 information such as personnel records, pupil records, medical records or financial information regarding any of its employees.

Accessing or attempting to access another's password, data, messages or other information without permission.

Downloading Files and Software

All computer files downloaded via e-mail attachment or in any other manner to CESA #9 electronic communication system or computer resources must be scanned for viruses. No software may be downloaded without proper authorization.

Child Internet Protection Act – Internet Safety Policy

It is the policy of CESA #9 to:

a) Prevent user access over its computer network to, or transmission of, inappropriate material via internet, electronic mail, or other forms of direct electronic communication;

b) Prevent unauthorized access and other unlawful on-line activities;

c) Prevent unauthorized on-line disclosure, use, or dissemination of personal identification information of minors; and

d) Comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 U.S.C. 254(h)].

Definitions

As used herein, the following terms have the following meanings ascribed to them.

Computer – The term "computer" includes any hardware, software, or other technology attached or connected to, installed in or otherwise used in connection with a computer.

Access to Internet – A computer is considered to have "access to the Internet" if the computer is equipped with a modem or is connected to a computer network which has access to the Internet.

Minor – The term "minor" means an individual who has not obtained the age of 17.

Child Pornography – The term "child pornography" has the meaning given such term in § 2256 of Title 18, U.S.C.

Harmful to Minors – The term "harmful to minors" means any picture, image, graphic image file or other visual depiction that: (1) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex or excretion; (2) depicts, describes or represents, in a patently offensive way with respect to what is suitable for minors; an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and (3) taken as a whole lacks serious literary, artistic, political or scientific value as to minors.

Obscene: The term "obscene" has the meaning given such term in § 1460 of Title 18, U.S.C.

Sexual Act; Sexual Contact – The terms “sexual act” and “sexual contact” have the meanings given such terms in § 2246 of Title 18, U.S.C.

Access to Inappropriate Materials

To the extent practical, technology protection measures (“internet filters”) shall be used to block or filter Internet or other forms of electronic communication access to inappropriate information.

Specifically, as required by the Children’s Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors.

Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bonafide research or other lawful purposes.

Inappropriate Network Usage

To the extent practical, steps shall be taken to promote safety and security of users of CESA #9 on-line computer network when using electronic mail, chat rooms, instant messaging or other forms of direct electronic communications.

Specifically, as required by the Children’s Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called “hacking” and other unlawful activities; and (b) unauthorized disclosure, use and dissemination of personal identification information regarding minors.

Supervision and Monitoring

It shall be the responsibility of all members of the CESA #9 staff to supervise and monitor usage of the on-line computer network and access to the Internet in accordance with this policy and the Children’s Internet Protection Act.

Procedures for the disabling and otherwise modifying any technology protection measures shall be the responsibility of CESA #9 Technology Department.

Tentative Approval: December 5, 2001

FINAL APPROVAL: January 2, 2002