

## APPROPRIATE USE OF COMPUTERS, COMPUTER NETWORK AND THE INTERNET- EMPLOYEES

The appropriate and equitable use of all types of District owned and maintained technology is a privilege not a right and must be consistent with the objectives of the District. Access to the District's computers, computer network systems and the Internet shall be available to staff within the District. Appropriate use of the District's technology to conduct work related activities is encouraged to enhance timeliness, effectiveness and productivity whenever possible. The District makes no guarantee as to the accuracy of information found on the Internet. Communication over the network is often public in nature and should be conducted in a professional manner.

Identified employees may be able to access the local and wide area networks of the District as appropriate to their positions. The amount of time and type of access available for each staff member may be limited by the District's technology resources and the demand for use of the District's technology. Individual computers may be equipped to access Internet. Individual staff e-mail accounts may be issued. Some sites on the Internet may contain material the District considers illegal, defamatory, inaccurate, offensive or pornographic. Every effort should be made to avoid accessing such sites. Employees' Internet activities will be monitored by District personnel to ensure that employees are not accessing inappropriate sites that include obscenity, pornography and child pornography or are harmful to minors. The District will use technology protection measures to guard against employee access of inappropriate sites.

Instruction in appropriate use of the Internet system will be available to the appropriate employees.

Included in the training will be discussion of:

- How to access the Internet and e-mail
- Appropriate use of Internet and e-mail
- Expectations for employee use
- Security issues, i.e., passwords and files on the computer
- Review of this policy

The District maintains the right to monitor any and all aspects of its computers, network systems and Internet access including, but not limited to, monitoring sites staff visit on the Internet and reviewing e-mail. The administration and the technology coordinator shall have both the authority and the right to examine all Internet activity including any logs, e-mail, computer disks and/or other computer related records of any user of the system. Staff waives any right to privacy in anything they create, store, send or receive on the District's computers and computer network systems, including the Internet. Each employee, who uses the District's computers, computer network systems and internet access, grants as a condition of that use any patent right to any invention created or associated with the use and/or any copyright to any materials created pursuant to that use.

Staff members shall only engage in appropriate, ethical and legal utilization of the District's computers, computer network systems and the Internet access. Staff members' use of the District's computers, network systems and the Internet shall comply with all District policies and regulations. Inappropriate use and/or access will result in the restriction and/or termination of this privilege and may result in discipline for staff members up to and including termination and/or legal action. The District's administration will determine what constitutes inappropriate use. The technology coordinator may close a user account at any time as required and administrators, faculty and staff may request the technology coordinator to deny, revoke or suspend user accounts. Any user identified as a security risk or having a history of problems

APPROPRIATE USE OF COMPUTERS, COMPUTER NETWORK AND THE INTERNET-  
EMPLOYEES

with other computer systems may be denied access to the District's computers, computer network and the Internet. Staff members will be provided a copy of this policy annually.

Legal References:                   Protection Act 47 U.S. C., Chapter 254 (h; Iowa Code Chapter) 279.9  
(1000)  
Iowa Penal Code, Chapter 716A

Cross References:                 605.6-Internet Acceptable Use Policy  
605.6E1-Internet Access Permission Letter to Parents  
605.6E2-Internet Appropriate Use Violation Notice  
605.6R1-Internet Appropriate Use Regulation

Approved: 1/08

Reviewed: 5/11, 2/13

Revised:

APPROPRIATE USE OF COMPUTER NETWORK AND THE INTERNET-EMPLOYEES

I. Responsibility for Internet Appropriate Use

A. The authority to enforce appropriate use of District technology resources is delegated to trained personnel and/or other adults designated and trained by the District.

B. All users are expected to practice appropriate use of District computers, computer networks and the Internet.

II. Employee Use of District Computers and/or Computer Network and the Internet

A. Employees must be efficient, ethical and legal in their use of the District technology resources.

B. Transmission of material, information or software in violation of any Board policy is prohibited.

C. Employees are prohibited from sending or soliciting sexually oriented messages or images.

D. Employees are prohibited from making or distributing illegal/unauthorized copies of software such as, but not limited to, software that has been downloaded or copied or is in the possession of the user without the appropriate registration or license.

E. Employees are prohibited from sharing a personal user account with anyone other than the network administrator.

F. Employees are prohibited from using instant messenger services, Internet Relay Chat or other forms of direct electronic communication or enter a chat room while using the District's computers, computer network systems or Internet connection unless authorized by the network administrator.

G. Employees are prohibited from vandalizing the District's computers or its computer network system including the use or attempted use of computer viruses or participation in hacking.

H. Employees are prohibited from using the District's computers and/or computer network for any commercial or for profit purposes, personal or private business, product advertisement or political lobbying.

I. Employees are prohibited from using the District's computers or computer network or stand-alone computer for any illegal activity.

J. Employees are prohibited from altering, modifying, corrupting or harming in any way the computer software and data files stored on the District's computers or computer network systems. Employees should not install any software on the hard drive of any District computer or on the District's computer network system or run any personal software from either floppy disk, CD-ROM or other storage media without prior permission and supervision from the appropriate technology staff.

K. Employees are prohibited from using any encryption software from any access point within the District.

## APPROPRIATE USE OF COMPUTER NETWORK AND THE INTERNET-EMPLOYEES

L. Employees are prohibited from downloading any programs from the Internet without prior permission from the District's technology coordinator or other appropriate personnel. Any programs downloaded from the Internet shall be strictly limited only to those that have received permission from the technology coordinator or assigned technology personnel.

### III. On Line Etiquette

A. It is the employee's responsibility to abide by the policies and procedures of any network that is being accessed. The use of the network may be taken away for violation of board policy or regulations.

B. Employees should adhere to online protocol

1. Respect all copyright and license agreements
2. Cite all quotes, references and sources
3. Adhere to reasonable time limits in gathering needed information or conducting business
4. Apply the same privacy, ethical and educational considerations utilized in other forms of communication

C. When accessing electronic mail, employees should adhere to the following guidelines:

1. No expectation of privacy is implied; private messages should be limited to educational or business usage
2. Delete unwanted messages immediately
3. Use of objectionable language is prohibited
4. Unauthorized use of another person's e-mail is strictly prohibited
5. Always sign messages when authorized to use another person's e-mail

### IV. Unauthorized Costs

If an employee gains access to any service via the Internet which has a cost involved or if an employee incurs other types of costs, the employee will be responsible for those costs.

Approved: 1/08

Reviewed: 5/11, 2/13

Revised: