COMPUTER USE POLICY (CUP)

The Computer Use Policy (CUP) defines the acceptable use of District networked and stand-alone hardware and software. A printed hard copy of this policy is available in the District Office as well as in the principal's office of each building.

This policy also includes a specific listing of appropriate user behaviors that apply to all student and staff users of District network resources. It is important for all users of the District's information technology to review and understand this policy and any regulations that apply to their work location.

The following is a list of specific system-use requirements that apply to all users of system-wide networked resources regardless of building, platform, operating system, and application.

1. Only District Technology Staff is authorized to make hardware or software configuration changes to any networked or stand-alone resources. These changes include:
   - The installation or de-installation of software applications.
   - The installation or de-installation of workstation or network hardware.
   - The removal, relocation, addition, or reconfiguration of any network element.

2. New software installations will not be made until the proposed software:
   - Has been recommended by content area experts.
   - Is approved by district Information Technology staff for network compatibility.
   - Is previewed by content area experts and district Information Technology staff.

3. Subject to the software review process, applications and other executable files may be installed on the server or workstation hard drive. Once installed, they will not be removed without additional software review.

4. The district Information Technology staff will identify network software, hardware, and other devices that will be supported district-wide. This list will be updated and published as necessary.

5. Users will be assigned network home (H) directories in which to store files created on the district system. These directories will be limited in size subject to the nature of their use. This is the only location where users should store data that users expect to be backed up by district Information Technology staff.

6. Files created and stored on the district system are subject to review by authorized district staff. These documents may also be subject to access as a result of formal Freedom of Information Law (FOIL) requests and other legally enforceable access requests.

7. Unauthorized access to any part of the district system is strictly prohibited and may result in the loss of system privileges, district-imposed discipline, or legal action.

8. Unless specifically authorized and enabled by district Information Technology staff, no data will be stored on a workstation hard drive (drive C), writeable CD, DVD, zip drive, or other storage or removable media other than the user's server-based home (H) directory.

9. Only the files stored on district servers may be backed up by district Information Technology staff. Since storage space is limited, users will be required to purge their files on a regular basis. With notice, district Information Technology staff may also remove files on a regular basis. An archiving option will be developed and offered to each user as files are purged from the respective "H" directory.

10. Generally, data can be read to and accessed from the workstation 3.5" floppy drive. Since floppy disk files are a ready source of viruses, the district may disable this access on a public access machines if it represents a virus threat.

11. Users will not access computer games from any source unless used as a part of teacher-supervised instruction or activity authorized by the building principal.

12. Only screen savers and wallpaper included in the current workstation operating system can be installed on the desktop. Unauthorized screen savers and wallpaper will be removed from a workstation before any maintenance or troubleshooting work is done on it.

13. Student and staff access to the district network for any purpose will be password controlled.

14. No executable files in any form will be downloaded from the Internet or other outside sources or installed or stored on any district resources. This restriction includes Hot Mail, AOL mail, Instant Messaging, or any other commercial, privately developed, locally developed, or experimental executable file, macro, or application.

15. The district will not maintain student e-mail accounts. The district will make e-mail accounts available to staff. Use of e-mail will be limited to that which is available through the district Point Of Presence (POP), which does not allow nor support Hot Mail. The use of any district-supplied e-mail account will be strictly limited to communication in support of the instructional, non-instructional, and administrative work of the district. Since all students do not have equal access to technology outside of school, the instructional application of electronic resources will be supplemental to, and not in lieu of, other district-supplied instructional resources.

16. All users of the district system are specifically prohibited from engaging in the following activities:

    - Sending or displaying offensive messages or pictures; i.e., pornography.
    - Using obscene language.
    - Harassing, insulting or threatening others.
    - Damaging computers, systems, or networks.

- Downloading or installing unapproved software or hardware.
- Violating copyright laws and the valid licensed rights of others.
- Using another user's password.
- Encrypting or password protecting material stored on the system.
- Possessing programs used for hacking or stealing passwords.
- Trespassing in another user's folders, work or files.
- Intentionally wasting limited resources.
- Employing the network for non-school related, commercial or other private purposes.
- Use of an account by anyone other than the account holder.
- Use of e-mail or other communication facilities by students or the personal use of e-mail, instant messaging and any use of Hot Mail (Yahoo, AOL, MSN)
- Requesting unnecessary and lengthy material that ties up system resources.

Implementation of the District's CUP

It is important that all users have the opportunity to review, ask questions about, and understand the Computer Use Policy. During each school year, the Computer Use Policy will be reviewed with all staff. Changes will be distributed as it is revised each year. New staff will have the opportunity to review this document and ask questions about its content during staff orientation.

In addition, each building principal will review the Computer Use Policy with the students of his or her building as it relates to prohibiting conduct outlined within the district's Code of Conduct.

Approved: October 5, 2004