Instructional Technology (Administrative Rule)
Technology Use Guidelines **Code #363.00AR**

Network users are ultimately responsible for their actions in accessing network services and for adhering to the Tri-County Area School District technology use procedures. Therefore, users shall follow the rules of on-line behavior established by the District and conduct themselves in a manner consistent with other expected school behavior and district policies.

A signed independent internet user agreement and parent permission form for students or a signed Staff Instructional Technology User Agreement form for staff shall be on file before the user may have direct access to the technology resources or electronic mail.

1. Software/Hardware
   1.1. Software will not be installed to local hard drives or to any network shares/drives unless pre-approved by the Network Administrator. The Network Administrator may remove any unauthorized software.
   1.2. Staff wishing to purchase software/hardware must submit a Technology Hardware/Software Purchase Request to the Network Administrator for approval before it will be considered for purchase. This is to eliminate unnecessary duplication of resources and compatibility to the network/computer system.
   1.3. In an effort to be uniform, only Microsoft Windows operating system will be supported. Consequently, only lab software written for that platform will be purchased.
   1.4. No one except under the direction of the Network Administrator should attempt to reconfigure or repair any District computer.
   1.5. Student information should be saved to a USB Flash Drive or to the user's "W" (network) drive. Students are forbidden to save files to the local hard drive.
   1.6. Network users are forbidden to download files from the Internet unless they have an educational purpose and have been pre-approved by the Network Administrator. At no time should games, music files, screen savers, wallpapers, program executable files or any file deemed unacceptable be saved to the hard drive, the user's "W" drive or any network shares/drives.
   1.7. District network resources are not to be used to play Internet games, listen to streaming music, or to view steaming video unless they have an educational purpose and have been pre-approved by the Network Administrator.
   1.8. Copyrighted material may not be placed on any system connected to the District's network without the creator's permission.
   1.9. No one, except under the direction of the Network Administrator, should delete files from the local hard drive.

1.10. Only the user or Network Administrator should delete files from their "W" drive.
1.11. Staff and students are responsible for backing up their own data.
1.12. Technology hardware and software is to be respected at all times. Failure to use technology resources in an acceptable manner may result in loss of technology use privileges.
1.13. The District reserves the right to periodically view files stored on the local/network drives. If any files are saved on the local/network drive that does not meet the Technology Guidelines, the Network Administrator may delete them.
1.14. The District reserves the right to search user's removable media (USB flash drive, CD-ROM's or DVD-ROM's) if there is a reasonable suspicion that the media contains files or data that could be considered unacceptable or destructive to the network.

2. Security
2.1. Users are to log into the network using only their assigned username. Passwords should never be shared.
2.2. Staff and students should secure their workstation before leaving it. Students should logoff and staff should either lock down their workstation or logoff.
2.3. Students are not to use an instructor's machine without permission from the instructor. Tampering with files and configuration will result in suspension of technology use.
2.4. Any rewriteable media (USB flash drive, CD-ROM's or DVD-ROM's) should be scanned for viruses before using.
2.5. The anti-virus software should not be disabled or reconfigured in anyway.
2.6. Users are not to use any method to circumvent the Internet Filters.
2.7. Students using any technology resources must be monitored by district staff.
2.8. No student should be at a DOS prompt or in Windows Explorer unless he/she is under the direct supervision of an instructor.
2.9. Users are responsible for deleting unnecessary files from their home "W" drive. If a user abuses this privilege, server storage for that user may be restricted.
2.10. Network Folders of graduating seniors will be deleted upon graduation. Network Folders and Mailboxes of non-returning staff will be deleted after notification from school administrators. Network Folders of underclass student users will be emptied at the end of each school year.

3. Internet & Email Use
3.1. All users will abide by the Internet Safety and Acceptable Use Policy (#300-Code 367 & 367R).

3.2. Both Independent Internet Users and District Staff will be required to sign their respective User Agreements (#300- 363.2E1 Independent Internet User Agreement or #300- 363.2E2 Staff Instructional User Agreement) on an annual basis. These forms will be kept on file.
3.3. Users specifically agree not to submit, publish or display any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal material. Transmission of material, information or software in violation of any local, state, or federal law is prohibited.
3.4. Users must regularly delete mail from their mailboxes to conserve server storage space.
3.5. Users are not to use District resources to send objectionable material or to forward chain letter materials.
3.6. The District reserves the right to view email, archived email, Internet traffic, or any data sent over the network.

Consequences for Failure to Abide by Technology Guidelines

Students violating District Technology Guidelines will be subject to the following consequences:

First Offense: Verbal reprimand will be given by the building Principal or designee, and the violation will be documented in the student's file. The student will be monitored by District Staff and the Network Administrator for further violations for a timeframe determined by the building Principal or designee.

Second Offense: Student use of technology will be restricted to use for classroom purposes only, while under direct supervision of the classroom teacher. Parental contact will be made by the building Principal and the violation will be documented in the student's file. The issuance of a Second Offense will also result in moving up a step on the disciplinary scale. The student will continue to be monitored by District Staff and the Network Administrator for further violations for a timeframe determined by the building Principal or designee.

Third Offense: Technology privileges will be revoked for a period of time to be determined by the building Principal and the Network Administrator. Parental contact will be made by the building Principal and the violation will be documented in the student's file. The issuance of a Third Offense will also result in moving up a step on the disciplinary scale.

Depending on the seriousness of the violation, the progression of consequences may be accelerated by the building principal or designee with input from the Network Administrator

Depending on the seriousness of the violation, offenses can be carried over from year to year.

Staff violating District Technology Guidelines will be subject to disciplinary action by school officials.

Prior Approval:	August 25, 2009
Attorney Review:	December 2015
Approved:	January 26, 2016