Technology Resources User Guidelines

Acceptable Use--The use of the school's technology resources must be in support of education and research and consistent with the district's educational objectives. Technology resources not only include district owned computers and servers but all resources used in the infrastructure. The infrastructure includes the wired network as well as the wireless network and the utilization of bandwidth associated with each segment of the network.

Technology resources **may** be used for academic, school-related purposes: e.g. instruction, research, production.

Technology resources **may not** be used for the following non-academic purposes:

- playing non-educational games
- instant messaging
- excessive personal emailing or web surfing
- accessing social networking sites for personal use
- downloading and/or uploading non-school-related content

In addition, users **are prohibited from:**

- creating or using proxy websites to bypass the district's filtering (CIPA) program
- conducting a commercial business using the school's technology resources
- running programs designed to intercept packets or to disrupt the security or operation of the schools network
- participating in activities such as piracy—either the attainment or distribution of software or other copyrighted materials—over the school's network

Privileges—The use of the school's technology resources is a privilege, not a right, and inappropriate use will result in the cancellation of those privileges and/or disciplinary action. Disciplinary action will be taken according to due process outlined in the student handbook. The following privileges may be denied as a result of disciplinary action:

- Access to a user folder
- Access to printing
- Access to all productivity applications
- Access to the student information system
- Access to the library catalog
- Access to reference databases
- Access to the internet

If a student is denied these privileges due to disciplinary action, necessary accommodations for completion of classroom assignments will be made.

If a parent wishes to exclude their child from internet usage, it should be indicated on the student registration card.

Etiquette—Users are expected to abide by the generally accepted rules of network etiquette. Users are not to modify the standard configuration of any computer. Users must login and logout from the network properly. Users should report any malfunction to the appropriate staff. Users should not use the network in any way that disrupts use by others.

Email—User use of non-academic related email should be kept to a minimum. Messages relating to or in support of illegal activities may be reported to the proper authorities. Illegal activities are strictly forbidden. This includes but is not limited to threats, harassment, stalking and fraud.

Intellectual Property—Users must respect the intellectual property of others by crediting sources and following all copyright laws. Users may not download or install software on school computers.

Network Accounts—Users are assigned a network account login which may be used on any computer in the school. The login gives users access to printers and resources. It also gives users storage space on the building file server. This space may only be used to store documents created for school-related projects. Users may not use the network to store programs or applications of any type, or non-school-related projects. Files stored in users' accounts are not guaranteed to be private. School staff may review the contents of user accounts to maintain system integrity and ensure responsible and appropriate use. Inappropriate use of user accounts may result in disciplinary actions, including loss of computer access privileges.

Personal Computers Using Network—Users are permitted to access the school's wired and wireless network with their own computers, however the same acceptable use guidelines are in effect. Users may not engage in activities that consume excessive amounts of network bandwidth, such as downloading, uploading and/or live streaming non-school-related content. If network administrators suspect high utilization of bandwidth or inappropriate use of district technology resources, a user may be asked to turn over a device and any passwords needed to verify the suspicions.

Security—Security on the computer network is imperative. Specific actions are prohibited:

- Using another user's account without permission.
- Sending network broadcast messages, thereby disrupting network use by others.
- Attempting to breach the desktop security of a computer.
- Attempting to break into password protected areas of a network or tampering with network systems.
- Accessing unauthorized portions of the student information system.
- Inappropriately messaging through the student information system.

Any user identified as a security risk may be denied access to the school's technology recourses.