Acceptable Use of Technology and Electronic Resources
USD #480 Employee Agreement

I. Definitions

The term "Network" for purposes of this policy shall include (i) all hardware and software provided by the District to employees or students for their use; (ii) internet and internet access provided by the District; (iii) computer system provided by the District; (iv) all the Network provided by the District; (v) all electronic mail and communication access provided by the District (communications); and all electronic research access provided by the District. The district provides computer network and internet access for its students and employees. This service allows employees and students to share information, learn new concepts, research diverse subjects, and create and maintain school-based websites. The district has adopted the following Acceptable Use Guidelines to govern the conduct of those who elect to access the computer network or district Internet.

II. Electronic Communication Use

Users shall adhere to the following guidelines of acceptable use:

1. Use of the network/internet is in support of educational objectives of USD 480.
2. Users are not permitted to obtain, download, view or otherwise gain access to pornography, obscene depictions, or other materials harmful to minors. Use of the network for creation, dissemination, or viewing of defamatory, factually inaccurate, abusive, obscene, profane, sexually oriented, threatening, harassing, or other material prohibited by law or district policy.
3. Email**,** messages, and instant messaging (electronic communication) exchanged through the network shall meet the educational objectives of USD #480. Personal use of the network should be limited and shall not interfere with the user's district responsibilities.
4. Users should assume all communications, information and network traffic are public when transmitted via the network and may be viewed by others. System administrators may access and read email on a random basis without notice.
5. The network is not to be used for commercial or business activities, political lobbying, and/or personal promotion.
6. The use of obscene, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, harassing, offensive, or prejudicial language is prohibited. Restrictions against inappropriate language apply to all file or document names, electronic communication, and material posted on the Web.
7. Users will promptly disclose to the building principal or Director of Technology any messages or information received that is inappropriate or makes them feel uncomfortable.

III. Hardware/Software Use

1. Use only software that is approved by the Director of Technology on all workstations and the network. Other software/disks are not allowed. Loading software from disks or the Internet is prohibited. Users will abide by all software licensing agreements.
2. No personal device can be connected to the network unless it meets BYOD policy. All district Technology devices must be pre-approved by Director of Technology before purchase.
3. All hardware and software used in the district is considered property of the district. Users may not damage, alter, modify the equipment or software or access, delete, copy, modify, nor forge others users' e-mails, files or data, including iCloud logins for iPads.
4. Users will not remove, uninstall or logout of any district installed software.
5. Users may not claim personal copyright privileges over files, data, or materials for USD #480. All right, title and interest of every kind and nature, whether now known or unknown, in and to any files,

data, materials, ideas or creations created, written developed or produced during the term of employee's employment with the district, whether or not during working hours, that are within the scope of the districts operations or relate to any of the district's activities or projects shall be the exclusive property of the district.

6. Users shall not use copyrighted materials without the permission of the copyright holder (Ex: Downloading YouTube Videos).
7. Users shall not in any way attempt to introduce computer code designated to self-replicate, damage, or otherwise hinder the performance of the network (Ex: bug, virus, worm, or similar name).
8. Users shall not attempt to gain unauthorized access to the network or to any other computer system through the network or go beyond authorized access. This activity may be considered "hacking" (Ex: MiFi, Proxy, Hotspot).

IV. Network Security

1. Users will immediately notify the building principal or Director of Technology if they have identified a possible security or operating problem.
2. Users shall not let other persons use their name, logon, password, or files for any reason (except for authorized staff members), and users shall not use or try to discover another user's password.
3. **Users should not give their home address, personal phone number or any personal information about themselves or any student or school personnel to anyone.**
4. **It is all USD 480 staff members' responsibility to educate students about appropriate online behavior, including interactions with other individuals on social networking sites/chat rooms, and cyber bullying awareness and response.**
5. **It is all USD 480 staff members' responsibility to monitor student's online activity for appropriate behavior, which includes monitoring of iPad Logins.**
6. **USD 480 deploys an internet filtering system to monitor and restrict students and staff access to harmful materials, including viruses, malware and explicit content.**
7. **Any website "White List" request needs to get approval by building Administration and Director of Technology.**

V. Violation of Agreement

1. The use of the network, district technology and district electronic resources are a privilege and not a right. The school district has the right to make the determination of what constitutes inappropriate use and use as an educational tool.
2. Inappropriate use of district technology, the network or district electronic resources, or a violation of this Agreement, may result in one or more of the following consequences but not limited to:
   A. Removal of files by the district.
   B. Limitation of the user's right of access and use.
   C. Cancellation of the user's privileges.
   D. Disciplinary action, up to and including termination.
   E. Referral of the user and the user's activities to appropriate law enforcement agencies.
3. Staff/Students must properly care for and protect the district devices. My signature below indicates my acceptance of all financial responsibilities for the devices in my classroom and those provided to me by the district as outlined below:

   Devices assigned to Staff/Students:

   - 1st incident of damage to device: $100
   - All subsequent incidents of damage to device: full replacement cost
   - Lost, stolen: full replacement cost

   Damage to Devices in my classroom:

- Promptly upon noticing, or being told of, damages to devices in my class, staff will contact the building principal and will assist the building principal in determining who is responsible for such damages.

Staff Signature: _____ Date: _____

Signature indicates that the staff member has read and agrees to the above-mentioned guidelines, as well as all guidelines included in Board of Education Policy IFCC, and understands their obligations concerning the use of computers or networks for the duration of their employment with the district.

Revised 3-20-18