Maroa-Forsyth Unit District 2
Acceptable Use Policy for Access of Electronic Network

Acceptable Use: Access to the District's Internet and Computers, must be for the purpose of education, research, legitimate school business purpose, and be consistent with the educational objective of the District. Use is a privilege and not a right.

Material or information considered to be in violation of the AUP includes, but is not limited to the following:

a. Using the network for illegal activity, including violation of copyright, or other contracts or transmitting any material in violation of U.S. or State Law;

b. Unauthorized downloading of software, regardless of whether it is copyrighted or devirused;

c. Downloading copyrighted material for other than personal use;

d. Using the network for private financial or commercial gain;

e. Wastefully using resources, such as file space;

f. Hacking or gaining unauthorized access to files, resources, or entities;

g. Invading the privacy of individuals, which includes the unauthorized dissemination, and use of information about anyone that is of a personal nature;

h. Using another's account or password;

i. Posting material authorized or created by another without his/her consent;

j. Posting anonymous messages;

k. Using the network for commercial or private advertising;

l. Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material; and

m. Using the network while access privileges are suspended or revoked.

In addition, advertisement of products or services not directly related to the district fundraising functions is also prohibited.

Privileges: The use of electronic information resources is a privilege, not a right. Inappropriate use of these resources will result in disciplinary action and/or referral to legal authorities by school administrators. The principal will make all decisions regarding whether or not a user has violated any privileges and may deny, revoke, or suspend access at any time. The principal's decision is final.

You are responsible for your actions and activities involving the network. Some examples of unacceptable uses are:

-Using the network for any illegal activity
-Using another user's account or password
-Invading the privacy of individuals
-Posting material authored or created by another without his/her consent
-Accessing, downloading, or posting defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material
-Using the network for private or financial gain
-Posting anonymous messages
-Using the network while access privileges are suspended or revoked.

Network Etiquette: You are expected to abide by the generally accepted rules of the network etiquette. These include, but are not limited to, the following:

-Have good manners, be polite
-Always obey copyright laws
-Never knowingly post or forward information that is not true
-Ask for help when you need it
-Do not reveal personal addresses or telephone numbers of students or colleagues
-Do not us the network in anyway that would disrupt its use by others
-Treat people you meet on the Internet as if they were honored guests at your school
-Use appropriate language. Do not swear, or use vulgarities or any other inappropriate language.
-Recognize the electronic mail is not private. People who operate the system have access to all mail. Messages relating to or in support of illegal activities may be reported to authorities.

Security Network: Security if a high priority. If you can identify a security problem on the Internet, you must notify your teacher and/or school administrator. Any user identified as a security risk may be denied access to the network. Do not use another individual's account or log on to the system as the systems administrator.

Information stored on the network is not to be considered permanent or private. As such, the district retains the right to review and remove as needed data or files found on the network that violates the AUP or that are not in direct support of education or business. In addition, regular maintenance activities can result in the deletion of information deemed not compliant with the AUP.

When suspicion of a violation of the AUP pertaining to inappropriate material or usage exists, the district reserves the right to review data and files found on the network during the course of the investigation. Any information gained through this review may be used as evidence in disciplinary or legal action should a violation of the AUP exist.

Internet: Any employee/student who publishes to the district web server must do so with the permission of the technology director. All items posted on the district web server will become property of the school district.

It is advised to not reveal personal information, such as home address, phone numbers, passwords, credit card numbers, or social security numbers; this also applies to others' personal information or that of organizations. **The use of pictures without identifying information may be used from time to time on the school district website unless parents specifically state in writing to the school principal not to do so.**

Personal Computers: Unit 2 provides PC's to staff members and students on an as needed basis. District provided computers are not to be modified in any way, including the addition or removal of hardware or software, without the permission of the Director of Technology. District provided computers may not be removed from district property without prior approval. Removal of district owned equipment is in violation of the AUP and disciplinary or legal action may result.

District provided computers are not to be used for financial gain at any time. Use of district provided computers or systems to gain personal income or monies is expressly forbidden, unless it is for fundraising activities associated with the school and has prior approval. This activity is considered a violation of the AUP and subject to disciplinary or legal action.

Email: Email provided to the staff of Unit District 2 is primarily for internal and external business communications. Email addresses are not, except upon request, considered private and should be available to the public as deemed appropriate by the administration. Personal use of Unit 2 email resources is allowed, but should not interfere with the day-to-day duties of staff provided with district provided email resources, nor should it violate either the board of education's policies or the following four points:

-Staff use of email should not promote, or support political functions or agenda's in any way, both internally and externally.
-Staff use of email should not promote, or support private business or industry especially the originators own private concern or business.
-Staff use of email should not promote illegal activities or activities prohibited by district policy as found in this document or in the Board of Education Policy Manual.
-Staff shall not engage in internal or external email activities that are regarded as SPAM or mass emailing, unless for information purposes as approved by the district administration.

SPAM is defined as email that is sent to multiple individuals in an uninvited manner for the purpose of furthering a private or political agenda, the transmission of questionable material, or a means of solicitation.

It must be the student and staff's understanding that district provided email is not private or protected.

When suspicion of a violation of the AUP pertaining to inappropriate material or usage exists, either through discovery as part of regular maintenance or by staff complaint, the district reserves the right to review data and files found on email clients and servers during the course of investigation. Any information gained through this review may be used, as evidence in disciplinary or legal action should a violation of the AUP exist.

Vandalism: Vandalism is defined as any malicious attempt to harm or destroy property of the user, another user, or any other agencies or networks that are connected to the network as well as the Internet system. Vandalism also includes, but is not limited to overloading data on the server as well as uploading, downloading, or creation of computer viruses in an intentional manner. Vandalism is considered a violation of the AUP and as such is subject to disciplinary or legal action as deemed appropriate by the administration.

Service Disclaimer: Unit District 2 makes no warranties of any kind, whether expressed or implied, for the service it is providing. Unit 2 will not be responsible for any damages the employee or student may suffer while on this system.

These damages may include but are not limited to: loss of data as a result of delays, non-deliveries, mis-deliveries, or service interruptions caused by the system or by employee error or omission.
Use of any information obtained via the information system is at the employee's own risk. Unit 2 specifically denies any responsibility for the accuracy of information obtained through electronic information resources.

Filtering, Monitoring, and Review: Unit District 2, in order to comply with local, state, and federal laws and standards, filters the Internet content on systems that students may have access to. This filtering removes access to websites and Internet servers that have been deemed to have inappropriate content not of an educational value. Report any errors found regarding what sites being or not being filtered to an administrator or the Director of Technology.

Unit 2 retains that right to monitor network, email, computer, and telephone use without warning or notice. Information stored, transmitted, or communicated on Unit 2 equipment is not to be considered private. Information gained through monitoring may be used as evidence in disciplinary or legal action, at the administrations' discretion.

Unit district 2 retains the right to review current and back up copies of electronic systems, files, data, communications, and email. Reviews are done without notice, and information gained through review may be used as evidence in disciplinary or legal action should a violation of the AUP be discovered.

Authorization for Electronic Network Access: Each staff member must sign the District's **Acceptable Use Policy for Electronic Network Access** as a condition for using the District's electronic network. Each student and his or her parent(s) or guardian(s) must sign the **Acceptable Use Policy** before being granted unsupervised use.

No Warranties: The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages. This includes the loss of data resulting from delays, non-deliveries, missed deliveries, or service interruptions caused by its negligence or the user's errors or omissions. Use of any information obtained via the Internet is at the users own risk. The District specifically denies responsibility for the accuracy or quality of information obtained through its services.

Indemnification: The user agrees to indemnify the School District for any losses, costs, or damages including reasonable attorney fees, incurred by the District relating to, or arising out of, any breach of this Acceptable Use Policy.

User Signature Agreement:

I understand any violations of the above provisions of this Acceptable Use Agreement, when using the district electronic information resources, may result in the loss of my user account and in disciplinary and or legal action. I therefore agree to maintain the required standards and to report any misuse of the electronic information resources to a systems administrator.

I also agree to fully disclose to my administrator/supervisor all Internet/Intranet publishing activities on school network systems and web servers.

Misuse may include, but not limited to: Any messages information or graphics sent or intentionally received that include/suggest pornography; unethical or illegal solicitation, racism, sexism, inappropriate language; and other listings as described above.

Penalties may be but are not limited to the following:

-30 days off district network/communications system
-1 semester off district network/communications system
- 1 year off district network/communications system
-Permanent loss of district network/communications system

A person may also be suspended or removed from the school on a permanent basis in addition to the above penalties. Legal action may also be taken against a person violating the Acceptable Use Agreement.

I have read this agreement and understand that Internet sites are filtered and that my district electronic information resource accounts, files, and telephone resources may be monitored or reviewed. I hereby agree to comply with the above-described conditions of acceptable use.

USER NAME (print)_____

User signature_____

Parent signature_____

Date_____

Received for File_____