TURKEYFOOT VALLEY AREA SCHOOL DISTRICT

No. 815.1

SECTION: OPERATIONS

TITLE: ACCEPTABLE STUDENT USE OF INTERNET

ADOPTED: FEBRUARY 15, 2016

REVISED:

	815.1 ACCEPTABLE STUDENT USE OF INTERNET
1. Purpose	The Board supports the use of the Internet and other computer networks in the District's instructional program in order to facilitate learning and teaching through interpersonal communications access to information, research, and collaboration. The Internet within the school district has not been established for public access or public forum. The district has the right to place reasonable restrictions on the material that is accessed or posted. The Internet may not be used for commercial purposes to offer, provide or purchase products or services, nor may the system be used for political lobbying. Student use of the Internet under the auspices of the district is contingent upon conditions set forth in this policy.
2. Authority	The electronic information available to students does not imply endorsement of the content by the Turkeyfoot Valley Area School District, nor does the District guarantee the accuracy of information received on the Internet. The District shall not be responsible for any information that may be lost, damaged or unavailable when using the network or for any information that is retrieved via the Internet. The District shall not be responsible for any unauthorized charges or fees resulting from access to the Internet. The District reserves the right to log network use and to monitor fileserver space utilization by District (student) users, while respecting the privacy rights of both District users and outside users.
3. Delegation of Responsibility	Every student member has a responsibility to use the District's electronic network in a productive and ethical manner. Students has the responsibility to respect and protect the rights of every other user in the District and on the Internet.
4. Guidelines	Network accounts will be used only by the authorized owner of the account for its authorized purpose. All communications and information accessible via the network should be assumed to be private property and shall not be disclosed. Network users shall respect the privacy of the other users on the system. To the extent practical, technology protection measures (or Internet filters) have been implemented to block or filter Internet content or other forms of electronic

communications that is inappropriate for the stated educational goals and objectives of the district.

Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors.

In addition, the district will educate students about appropriate online safety including cyberbullying, interacting with other on social networking sites and in chat rooms, and in any other forms of electronic communication. The district will also monitor the online activity of minors through classroom observation and monitoring tools.

Subject to staff supervision, technology protection measures may be disabled, or in the case of minors, minimized only for preapproved educational research or other lawful purposes that are in accordance with the district's educational goals and objectives.

Users of the district network must abide by the following responsibilities:

1. Never share your password or account with anyone. You have full responsibility for the use of your account. All violation of this policy that can be traced to an individual account name will be treated as the sole responsibility of the owner of that account. Under no conditions should you give your password to another user.

2. Do not knowingly degrade the performance of the network. The creation, and/or distribution of destructive software, including, but not limited to, virus', Trojan horse, and worm programs, is strictly prohibited.

3. Obey the rules of copyright. Students must respect all copyright issues regarding software, information, and attributions of authorship. Commercial software may not be installed on the system without express permission of the Technology Department.

4. Use of the network for any illegal activities is prohibited. Illegal activities include tampering with computer hardware and software (hacking), unauthorized entry into computers, or knowledgeable vandalism or destruction of computer files. Such activity is considered a crime under state and federal law.

5. Use appropriate language. Profanity or obscenity will not be tolerated on the network. All students should use language appropriate for school situations as indicated by the Code of Student Conduct.

6. Avoid offensive or inflammatory speech. Personal attacks are unacceptable use of the network. If you are the victim of flame or slam, bring the incident to the attention of a teacher or administrator.

7. Impersonations, anonymity, aliases or pseudonyms are not permitted. As an educational network, we believe that individuals must take responsibility for their actions and words.

8. Exemplary behavior is expected on virtual field trips. When visiting locations on the Internet, or using the videoconferencing or screen sharing communication tools, students must conduct themselves as representatives of both their class and the entire school as a whole. Conduct that is in conflict with responsibilities outlined in this document will be subject to loss of network privileges.

9. Users should never reveal their names, home addresses, or personal phone numbers or the names of anyone else that they know on social networking sites, websites, chat rooms, etc.

24.P.S. 4601 et seq
20 U.S.C.6777
47 U.S.C. 254
24 P.S.1303.1-A
24 P.S. 4601 et seq
47 U.S.C. 254

The use of the district network for illegal, inappropriate or unethical purposes by students is prohibited. More specifically:

1. Use of the network to facilitate illegal activity is prohibited.

2. Use of the network for commercial or for-profit purposes is prohibited.

3. Use of the network for non-school purposes is prohibited.

4. Use of the network for product advertisement or political lobbying is prohibited.

5. Malicious use of the network to develop programs that harass other users or infiltrate a computer system and/or damage the software components of a computer or system is prohibited.

6. Hate mail, harassment, discriminatory remarks, and other antisocial communications on the network are prohibited.

7. The illegal installation, distribution, reproduction, or use of copyrighted software on district computers is prohibited.

8. Use of the network to transmit material likely to be offensive or objectionable to recipients is prohibited.

9. Use of the network to access obscene or pornographic material is prohibited.

10. Use of the network to intentionally obtain or modify files, passwords or data belonging to other users is prohibited.

11. Use of the network to misrepresent other users on the network is prohibited.

12. Use of district technology or the network for fraudulent copying, communications or modification of materials in violation of the law is prohibited and will be referred to the appropriate authorities.

13. Loading or use of unauthorized games, programs, files or other electronic media is prohibited.

14. The network shall not be used to disrupt the work of the others; and the hardware or software of other users shall not be destroyed, modified or abused in any way.

15. Use of the network which results in any copyright violation is prohibited.

16. Never use another person's password to gain access to the network.

Security

Security on any computer system is a high priority. If any network user identifies a security problem, s/he must notify the system administrator or a teacher at once without discussing it or showing it to another user. The user may not use another individual's account. Any user identified as a security risk will be denied access to the network.

Consequences

A network user shall be responsible (including financially) for damages to the equipment, systems or software resulting from deliberate or willful acts.

Failure to follow the procedures and prohibitions listed above may result in the loss of the right to access the network. Other appropriate disciplinary procedures may take place, as needed, for students.

The district has implemented an electronic procedure for monitoring student acceptance of this policy. Failure to accept the policy will deny a user access to the network.

Illegal use of the network, intentional deletion or damage to files of data belonging to others; copyright violations or theft of services will be reported to the appropriate legal authorities for possible prosecution.

Limitations of Liability

The district makes no warranties of any kind, whether express or implied, for the service it is providing. The district will not be responsible for any problems suffered while on the Internet. These problems include but are not limited to loss of data as interruptions, etc. Use of any information obtained through the Internet is at the user's own risk. The district does not accept responsibility for the accuracy of any data obtained on the Internet.

The district is also not responsible for any Internet content accessed by personal devices on networks that may overlap with our network's footprints (i.e. personal wireless networks, phone networks, etc.)

	Reference Policy 815, 814, 249, 224, 218