COMPUTER-ASSISTED INSTRUCTION
Internet Safety

It is the policy of this School District that to the extent reasonably possible, the staff and students will be encouraged and permitted to utilize the computer network provided by the School District for the purpose of facilitating learning and providing the best educational experience possible for its students. In this regard, the School District has made available to staff, electronic mail and the Internet. To gain access to the Internet, all students under the age of eighteen (18) must obtain parental permission and sign and return a parental permission form to the School District. Students eighteen (18) and over may sign their own forms. Access to the Internet will enable students to explore thousands of libraries, databases and bulletin boards while exchanging information with Internet users throughout the world. Families should be warned that some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate, or potentially offensive to some people. While it is possible for students to access inappropriate material and otherwise misuse the system, it is the intent of the School District that Internet access should only be used to further the educational goals and objectives set out for each student. It is the policy of this School District to educate our students using modern technology which the students will need to be familiar with in order to be successful in their 21st Century skills and careers. However, in order to utilize this modern technology, it will ultimately be the responsibility of parents and guardians of minors to set and convey standards to their children which they will follow while utilizing this technology. The School District will support and respect each family's right to decide whether or not to apply for access.

DISTRICT NETWORK ACCESS, INTERNET AND E-MAIL RULES.

Students and staff are responsible for good behavior on school computer networks just as they are in the classroom or a school hallway. Communicating on the network is often public in nature. General school rules for behavior and communications apply.

Internet filters shall be used to block access to obscenity, child pornography, and materials harmful to minors. Disciplinary action shall be taken against any student who tampers with the filters. The filters may only be disabled for bona fide research or other lawful purposes, and may only be disabled by the Internet coordinator or other faculty member or administrator.

INTERNET SAFETY TRAINING

In compliance with the Children's Internet Protection Act (CIPA) and the Protecting Children in the 21st Century Act, each year all District students will receive Internet safety training which will educate students about appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms, and cyberbullying awareness and response.

The network is provided for students to conduct research and communicate with others. Access to network services is given to students who agree to act in a considerate and responsible manner. Parental permission is required. Access is a privilege, not a right. Access entails responsibility. Individual users of the District computer networks are responsible for their behavior and communications over those networks. It is presumed that users will comply with District standards and will honor the agreements they have signed. Beyond the clarification of such standards, the District is not responsible for restricting, monitoring, or controlling the communications of individuals using the network.

Network storage areas are not to be considered private or personal property of students or staff. They are learning areas subject to review by administrators and teaching staff. Any files and communications may be reviewed by the administration or staff to maintain system integrity and to ensure that users are using the system responsibly. Users should not expect that files stored on District servers will be private.

While school teachers of younger students will generally guide them toward appropriate materials, older students and students utilizing the system outside of regular school hours will need to be directed by families in the same manner they direct their children's use of television, telephones, movies, radio, and other potentially offensive media.

Cyberbullying will not be tolerated. Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyberstalking are all examples of cyberbullying. Don't be mean. Don't send emails or post comments with the intent of scaring, hurting, or intimidating someone else. Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges. In some cases, cyberbullying can be a crime. Remember that your activities are monitored and retained.

The following conduct and utilization of the Intranet and Internet by students and staff are **NOT** permitted:

1. Sending or displaying offensive messages or pictures;

2. Using abusive, objectionable or obscene language;

3. Searching for, downloading, or otherwise reviewing any type of sexually explicit, obscene material or other information for any non-instructional or non-educational purpose;

4. Cyberbullying, harassing, insulting or attacking others;

5. Damaging computers, computer systems, or computer networks;

6. Violating copyright laws or otherwise using the network for any illegal purpose;

7. Using or attempting to discover another user's password nor shall user use or let others use another person's name, address, passwords, or files for any reason, except as may be necessary for legitimate communication purposes and with permission of the other person;

8. Trespassing in another's folders, work or files;

9. Intentionally wasting limited resources;

10. Employing the network for commercial purposes;

11. Otherwise accessing forums or "chat rooms" devoid of educational purpose;

12. Tampering with computers, networks, printers, or other associated equipment or software without the express permission of supervising staff;

13. Writing, producing, generating, copying, propagating or attempting to introduce any computer code designed to self-replicate, gather information from, damage, or otherwise hinder the performance of any computer's memory, file system or software.

14. While using school district computers and/or accessing school district web pages, or using the Internet service provided by the School District, user shall not engage in hacking, access unauthorized sites, or participate in any other unlawful activities online.

15. Disclosing, using or disseminating personal information regarding students.

EMAIL

Converse County School District #2 may provide users with email accounts for the purpose of school-related communication. Availability and use may be restricted based on school policies.

If users are provided with email accounts, they should be used with care. Users should not send personal information; should not attempt to open files or follow links from unknown or untrusted origin; should use appropriate language; and should only communicate with other people as allowed by the district policy or the teacher.

Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Email usage may be monitored and archived.

MOBILE DEVICES

Converse County School District #2 may provide users with mobile computers or other devices to promote learning outside of the classroom. Users should abide by the same acceptable use policies when using school devices off the school network as on the school network.

Users are expected to treat these devices with extreme care and caution; these are expensive devices that the school is entrusting to your care. Users should report any loss, damage, or malfunction to IT staff immediately. Users may be financially accountable for any damage resulting from negligence or misuse.

Use of school-issued mobile devices off the school network may be monitored.

PERSONALLY-OWNED DEVICES

Students should keep personally-owned devices (including laptops, tablets, smart phones, and cell phones) turned off and put away during school hours—unless in the event of an emergency or as instructed by a teacher or staff for educational purposes.

Because of security concerns, when personally-owned mobile devices are used on campus, they should not be used over the school network without express permission and instruction from staff. **USB/jump/flash drives are not to be used by students or staff without express consent from IT staff**. In some cases, a separate network may be provided for personally-owned devices.

SUPERVISION AND MONITORING

It shall be the responsibility of all District employees to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet Protection Act. Procedures for the disabling, filtering or otherwise modifying of any technology protection measures shall be the responsibility of the Technology Director or designated representatives. To make a request:

1. Follow the process prompted by the District's filtering software (or to remain anonymous, mail and anonymous request to the district's Technology Director; or

2. Submit a request, whether anonymous or otherwise, to the District's Superintendent/ the Superintendent's designee.

3. Requests for access shall be granted or denied within three (3) school days. If a request was submitted anonymously, persons should attempt to access the website requested after three (3) school days to see the status of the request.

4. Appeal of the decision to grant or deny access to a website must be made in writing to the building Principal stating the website that they would like to access and providing any additional detail the person wishes to disclose.

5. In case of an appeal, the building Principal will review the contested material and make a determination.

6. Material subject to the complaint will not be unblocked pending this review process.

In the event that a District student or employee feels that a website or web content that is available to District students through District Internet access is obscene, child pornography, or "harmful to minors" as defined by CIPA or material which is otherwise inappropriate for District students, the process described above should be followed. Any decision to filter or block web content will be made within thirty (30) days.

PENALTY

Violations will result in a loss of access as well as other disciplinary or legal action. The first offense will generally result in a warning and/or loss of technology privileges/Internet access until a parent conference, and further loss of privilege for such time as is determined by the administration. A second offense or a first offense of a flagrant nature, such as using the system for illegal behavior or intentionally damaging school district hardware or software, may result in removal from a class, termination of computer/network privileges, or recommendations for suspension and/or expulsion.

ADOPTED: May 9, 2013