Bond County CUSD#2 STUDENT Acceptable Use Policy
2016-2017

These guidelines are based on the Children's Internet Protection Act (CIPA) and its four guiding principles of: respect, privacy, sharing, and safety. These guidelines are appropriate for all technology users and we encourage parents to follow these guidelines in their own homes. Bond County CUSD#2 provides access to electronic resources that promote educational excellence, sharing of information, innovative instruction, and online communication to enhance 21st Century learners the ability to live and work in the global economy. Online communication constitutes email, Internet, blogging, any use of network resources, etc. BCCU#2's electronic resources include, but are not limited to all hardware, software, data, communication devices, printers, servers, filtered Internet access, and local and wide area networks.

Online communication is critical for today's learners to apply 21st Century Skills and employ tools such as interactive websites, blogs, video conferencing, podcasts, etc. which offer authentic opportunities for students to express and share information. To keep students safe and comply with the Children's Internet Protection Act (CIPA), the Acceptable Use Guideline is put in place and updated to accommodate for the many education and global changes to date. This Acceptable Use Guideline is written for all those who use school provided Network connections. These connections may be used for classroom blogs, student emails, podcast projects, interactive websites, and any other occasion students, teachers, or community members use school Network space. The following is a statement of rules and guidelines for the acceptable use of electronic information resources. These are provided to help understand what acceptable behaviors with the use of technology are. While these rules and guidelines detail acceptable use of electronic information resources anywhere, these are rules and guidelines under which all members of the BCCU#2 community (students and staff) will be held accountable.

USAGE GUIDELINE

BCCU#2 provides students and staff access to various electronic resources including a wide range of educational materials through Internet and computer online services. BCCU#2 uses content filtering technology in compliance with CIPA on all school computers with Internet access to protect against unacceptable web content. However, no web filtering technology is 100% safe. BCCU#2 realizes this fact and takes every effort to monitor online activity.

Student Safety. Do not send any message that includes personal information such as: home address, personal phone numbers and/or last name for yourself or any other person. Likewise, the staff is not permitted to post this information to public domains (i.e. class web page or Internet). Student pictures and/or work may be included on district/ school/ classroom websites without identifying captions unless the site is password protected.

Extended Safety K- 5. Teachers of students in grades K-2 will access appropriate websites for their students. Students in grades 3-5 may not attempt to access any Internet resource without the prior consent of the teacher.

Password Protection. Internet passwords are provided for each user's personal use only and are, therefore, confidential. Never share your password, steal or use another person's password. If you

suspect that someone has discovered your password, you should change it immediately and notify your teacher or administrator who in turn will notify the network administrator or the technology director. As words are easily hacked, when establishing a password one should keep in mind that strong passwords consist of a combination of upper and lowercase letters, numbers and symbols.

Privacy. E-mail is no more private than a postcard. Students and staff need to know that files stored on school computers are not private. Network and Internet access is provided as a tool for educational purposes only. The District has the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the computer network and Internet access including transmitted and received information. All information files are the property of the District and no user shall have any expectation of privacy regarding such files. Federal Law requires that all email sent and received be stored for a period of 'seven years'.

Online Etiquette. Follow the guidelines of accepted behaviors within the school handbook. Use appropriate language and graphics. Swearing, vulgarities, suggestive, obscene, belligerent, harassing, threatening or abusive language of any kind is not acceptable. Do not use school online access to make, distribute, or redistribute jokes, stories, cyber bullying, obscene material or material which is based on slurs or stereotypes relating to race, gender, ethnicity, nationality, religion, or sexual orientation.

Messaging. Teachers may incorporate: email, blogs, podcasts, video conferencing, online collaborations, Messaging, texting, Virtual Learning Environments and other forms of direct electronic communications (i.e. cell phones, cameras, other mobile computing devices) or Web 2.0 applications for educational purposes. Although teachers monitor student online activity, it is the direct responsibility of the user to comply with this acceptable use policy.

Blogging/Podcasting. Uses of blogs, podcasts or other Web 2.0 tools are considered an extension of the classroom. Whether at home or in school, any speech that is considered inappropriate in the classroom is also inappropriate in all uses of blogs, podcasts, or other Web 2.0 tools. Students using blogs, podcasts or other Web 2.0 tools are expected to act safely by keeping ALL personal information out of their posts. Comments made on school related blogs should follow the rules of online etiquette detailed above and will be monitored by school personnel. If inappropriate, they will be deleted. Never link to web sites from a blog without reading the entire article to make sure it is appropriate for a school setting.

Plagiarism/Copyright/Licensing. Plagiarism is the act of using someone else's words or ideas as your own. Students are required to give proper credit to all Internet sources used in academic assignments, whether quoted or summarized. This includes all forms of media on the Internet, such as graphics, movies, music, and text. Plagiarism of Internet resources will be treated in the same manner as any other incidences of plagiarism, as stated in the school handbook. In addition, all students and faculty must adhere to the copyright laws of the Unites States (P.L. 94-553) and the Congressional Guidelines that delineate it regarding software, authorship, and copying information. All students and faculty should also adhere to the Creative Commons licenses where the author/artist denotes what media may be shared, remixed, or reused.

Proxies. The use of anonymous proxies to get around content filtering is strictly prohibited and is a direct violation of this agreement.

Illegal Activities. Use of the network for any illegal activities is prohibited. Illegal activities include, but are not limited to: (a) tampering with computer hardware or software, (b) software piracy (c) unauthorized entry into computers and files (hacking), (d) knowledgeable vandalism or destruction of equipment, (e) deletion of computer files belonging to someone other than oneself, (f) uploading or creating of computer viruses, (g) distribution of obscene or pornographic materials, and (h) sexting. Such activity is considered a crime under state and federal law. Users must be aware that any illegal action carried out over the Internet will be reported to law enforcement officials for possible prosecution. Please be advised, it is a federal offense (felony) to break into any security system. Financial and legal consequences of such actions are the responsibility of the user (staff, volunteer, and student) and student's parent or guardian.

TERMS OF AGREEMENT

The Bond County Community Unit #2 Schools reserve the right to deny, revoke or suspend specific user privileges and/or to take other disciplinary action, up to and including suspension, expulsion (students), or dismissal (staff) for violations of these Guidelines. The District will advise appropriate law enforcement agencies of illegal activities conducted through the Bond County CUSD#2 Internet Connection. The District also will cooperate fully with local, state, and/or federal officials in any investigation related to any illegal activities conducted through the service. The school district and its representatives are not responsible for the actions of the users or the information they access.

INTERNET RELEASE FORM

In order for a student to access the Internet, a parent/guardian and the student must sign and return this consent form by (date).

____ I GIVE my permission to Bond County CUSD#2 to allow my child computer access to the Internet or online services and my child agrees to the usage guideline listed herein.

____ I DO NOT GIVE permission to Bond County CUSD#2 to allow my child computer access to the Internet or online services. Since the school cannot always prevent student access to such services, I have directed my child not to access the Internet or online services.

ELECTRONIC RELEASE FORM

___ I give permission to display my child's image
___ I give permission to display my child's voice.
___ I give permission to display my child's work

___ I do not want my child's image to be displayed
___ I do not want my child's work to be displayed.
___ I do not want my child's voice to be displayed

Parent Signature _____

Student Signature _____