STUDENT USE OF TECHNOLOGY

The Board of Trustees intends that technological resources provided by the district be used in a safe and responsible manner in support of the instructional program and for the advancement of student learning. All students using these resources shall receive instruction in their proper and appropriate use.

(cf. 0440 - District Technology Plan)
(cf. 1113 - District and School Web Sites)
(cf. 1114 - District-Sponsored Social Media)
(cf. 4040 - Employee Use of Technology)
(cf. 6163.1 - Library Media Centers)

Teachers, administrators, and/or library media specialists are expected to review the technological resources and online sites that will be used in the classroom or assigned to students in order to ensure that they are appropriate for the intended purpose and the age of the students.

The Superintendent or designee shall notify students and parents/guardians about authorized uses of district technology, user obligations and responsibilities, and consequences for unauthorized use and/or unlawful activities in accordance with this Board policy and the district's Acceptable Use Agreement.

District technology includes, but is not limited to, computers, the district's computer network including servers and wireless computer networking technology (wi-fi), the Internet, email, USB drives, wireless access points (routers), tablet computers, smartphones and smart devices, telephones, cellular telephones, personal digital assistants, pagers, MP3 players, wearable technology, any wireless communication device including emergency radios, and/or future technological innovations, whether accessed on or off site or through district-owned or personally owned equipment or devices.

Before a student is authorized to use district technology, the student and his/her parent/guardian shall sign and return the Acceptable Use Agreement. In that agreement, the parent/guardian shall agree not to hold the district or any district staff responsible for the failure of any technology protection measures or user mistakes or negligence and shall agree to indemnify and hold harmless the district and district staff for any damages or costs incurred.

(cf. 6162.6 - Use of Copyrighted Materials)

The district reserves the right to monitor student use of technology within the jurisdiction of the district without advance notice or consent. Students shall be informed that their use of district technology, including, but not limited to, computer files, email, text messages, instant messaging, and other electronic communications, is not private and may be accessed by the district for the purpose of ensuring proper use. Students have no reasonable expectation of privacy in use of the district technology. Students' personally owned devices shall not be

STUDENT USE OF TECHNOLOGY (continued)

searched except in cases where there is a reasonable suspicion, based on specific and objective facts, that the search will uncover evidence of a violation of law, district policy, or school rules.

(cf. 5145.12 - Search and Seizure)

The Superintendent or designee may gather and maintain information pertaining directly to school safety or student safety from the social media activity of any district student in accordance with Education Code 49073.6 and BP/AR 5125 - Student Records.

(cf. 5125 - Student Records)

Whenever a student is found to have violated Board policy or the district's Acceptable Use Agreement, the principal or designee may cancel or limit a student's user privileges or increase supervision of the student's use of the district's equipment and other technological resources, as appropriate. Inappropriate use also may result in disciplinary action and/or legal action in accordance with law and Board policy.

(cf. 5125.2 - Withholding Grades, Diploma or Transcripts)
(cf. 5144 - Discipline)
(cf. 5144.1 - Suspension and Expulsion/Due Process)
(cf. 5144.2 - Suspension and Expulsion/Due Process (Students with Disabilities))

The Superintendent or designee, with input from students and appropriate staff, shall regularly review and update procedures to enhance the safety and security of students using district technology and to help ensure that the district adapts to changing technologies and circumstances.

Internet Safety

The Superintendent or designee shall ensure that all district computers with Internet access have a technology protection measure that protects against access to visual depictions that are obscene, child pornography, or harmful to minors and that the operation of such measures is enforced. (20 USC 6777; 47 USC 254; 47 CFR 54.520)

To reinforce these measures, the Superintendent or designee shall implement rules and procedures designed to restrict students' access to harmful or inappropriate matter on the Internet and to ensure that students do not engage in unauthorized or unlawful online activities.

Harmful matter includes matter, taken as a whole, which to the average person, applying contemporary statewide standards, appeals to the prurient interest and is matter which depicts or describes, in a patently offensive way, sexual conduct and which lacks serious literary, artistic, political, or scientific value for minors. (Penal Code 313)

STUDENT USE OF TECHNOLOGY (continued)

The district's Acceptable Use Agreement shall establish expectations for appropriate student conduct when using the Internet or other forms of electronic communication, including, but not limited to, prohibitions against:

1. Accessing, posting, submitting, publishing, or displaying harmful or inappropriate matter that is threatening, obscene, disruptive, or sexually explicit, or that could be construed as harassment or disparagement of others based on their race/ethnicity, national origin, sex, gender, sexual orientation, age, disability, religion, or political beliefs

(cf. 5131 - Conduct)
(cf. 5131.2 - Bullying)
(cf. 5145.3 - Nondiscrimination/Harassment)
(cf. 5145.7 - Sexual Harassment)
(cf. 5145.9 - Hate-Motivated Behavior)

2. Intentionally uploading, downloading, or creating computer viruses and/or maliciously attempting to harm or destroy district equipment or materials or manipulate the data of any other user, including so-called "hacking"

3. Distributing personal identification information, including the name, address, telephone number, Social Security number, or other personally identifiable information, of another student, staff member, or other person with the intent to threaten, intimidate, harass, or ridicule that person

The Superintendent or designee shall provide age-appropriate instruction regarding safe and appropriate behavior on social networking sites, chat rooms, and other Internet services. Such instruction shall include, but not be limited to, the dangers of posting one's own personal identification information online, misrepresentation by online predators, how to report inappropriate or offensive content or threats, behaviors that constitute cyberbullying, and how to respond when subjected to cyberbullying.

Legal Reference: (see next page)

STUDENT USE OF TECHNOLOGY (continued)

Legal Reference:
EDUCATION CODE
49073.6 Student records; social media
51006 Computer education and resources
51007 Programs to strengthen technological skills
60044 Prohibited instructional materials
PENAL CODE
313 Harmful matter
502 Computer crimes, remedies
632 Eavesdropping on or recording confidential communications
653.2 Electronic communication devices, threats to safety
UNITED STATES CODE, TITLE 15
6501-6506 Children's Online Privacy Protection Act
UNITED STATES CODE, TITLE 20
6751-6777 Enhancing Education Through Technology Act, Title II, Part D, especially:
6777 Internet safety
UNITED STATES CODE, TITLE 47
254 Universal service discounts (E-rate)
CODE OF FEDERAL REGULATIONS, TITLE 16
312.1-312.12 Children's Online Privacy Protection Act
CODE OF FEDERAL REGULATIONS, TITLE 47
54.520 Internet safety policy and technology protection measures, E-rate discounts
COURT DECISIONS
New Jersey v. T.L.O., (1985) 469 U.S. 325

Management Resources:
CSBA PUBLICATIONS
Cyberbullying: Policy Considerations for Boards, Policy Brief, July 2007
FEDERAL TRADE COMMISSION PUBLICATIONS
How to Protect Kids' Privacy Online: A Guide for Teachers, December 2000
WEB SITES
CSBA: http://www.csba.org
American Library Association: http://www.ala.org
California Coalition for Children's Internet Safety: http://www.cybersafety.ca.gov
Center for Safe and Responsible Internet Use: http://csriu.org
Federal Communications Commission: http://www.fcc.gov
Federal Trade Commission, Children's Online Privacy Protection:
http://www.ftc.gov/privacy/privacyinitiatives/childrens.html
U.S. Department of Education: http://www.ed.gov

STUDENT USE OF TECHNOLOGY

Introduction

McCabe Union Elementary School District believes that access to technology in school gives students greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. We are committed to helping students develop the technology and communication skills that are necessary to support their future success. Therefore we believe all students should have access to technology tools when they act in a safe, responsible, courteous and legal manner.

The District Acceptable Use of Technology Agreement outlines the guidelines and behavior that students are expected to follow when using school technologies or when using personally owned devices on the school campus.

The McCabe Union Elementary School District network is intended for educational purposes. All activity over the network or while using district technologies will be monitored and may be retained. Access to online content via the network is restricted through filtering in accordance with our policies and federal regulations, such as the Children's Internet Protection Act (CIPA). Students are expected to follow the same rules for good behavior and respectful conduct online as offline. Misuse of school resources can result in disciplinary action.

McCabe Union Elementary School District makes a reasonable effort to ensure students' safety and security online, but will not be held accountable for any harm or damages that result from use of school technologies.

Student users of the district network or other technologies are expected to alert school staff immediately of any concerns for safety or security. McCabe Union Elementary School District will not be held accountable for any harm or damages resulting from student violations of copyright restrictions or user mistakes or negligence.

Technologies Covered

McCabe Union Elementary School District may provide internet access, desktop computers, mobile computers, handheld devices, videoconferencing capabilities, online collaboration capabilities, message boards, email, and more. Teachers and students may be using newer Web tools such as blogs, wikis, podcasts, and videocasts. These technologies improve student communication and collaboration skills, provide a real audience, and extend learning beyond the classroom walls while building digital citizenship skills. As new technologies emerge, McCabe will attempt to provide access to them. The policies outlined in this document are intended to cover all available technologies, not just those specifically listed.

STUDENT USE OF TECHNOLOGY (continued)

Usage Policies

All technologies provided by the district are intended for education purposes. Students are expected to be safe, appropriate, careful and kind; students should not try to get around technological protection measures; they should ask if they don't know.

Web Access

McCabe Union Elementary School District provides students with access to the internet, including web sites, resources, content, and online tools. That access will be restricted in compliance with CIPA regulations and school policies. Web browsing may be monitored and web activity records may be retained indefinitely. Users are expected to respect that the web filter is a safety precaution, and should not try to circumvent it when browsing the web. If a site is blocked and a student believes it shouldn't be, the student should alert the teacher.

Social/Web 2.0 / Collaborative Content

Recognizing the benefits that collaboration brings to education, McCabe Union Elementary School District may provide students with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users. Posts, chats, sharing, and messaging will be supervised and monitored by teachers. Students are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Students should be careful to never share personally-identifying information online.

Mobile Devices Policy

McCabe Union Elementary School District may provide students with mobile computers or other devices to promote learning in the classroom. Students are expected to treat these devices with extreme care and caution; these are expensive devices that the school is entrusting to your care. Students should report any loss, damage, or malfunction to the teacher immediately.

Personally-Owned Devices Policy

Students must 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 may not be used over the school network without express permission from staff.

Security

Students are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin. If a student

STUDENT USE OF TECHNOLOGY (continued)

believes a computer or mobile device might be infected with a virus, they should alert a teacher. Students should not attempt to remove the virus or download any programs to help remove the virus.

Downloads

Students should not download or attempt to download any files, programs, or software updates, or run .exe programs over the school network or onto school resources, even if prompted to do so by the computer or device being used. Teachers may give students special permission to download images or videos. For the security of the network, such files should only be downloaded from sites provided by the teacher, and only for education purposes.

Netiquette

Students should always use the Internet, network resources, and online sites in a courteous and respectful manner. Students should also recognize that among the valuable content online is unverified, incorrect, or inappropriate content. Trusted sources should be used when conducting research via the Internet. Teachers or library staff can help with this.

Plagiarism

Students should not plagiarize (or use as their own, without citing the original creator) content, including words or images, from the Internet. Students should not take credit for things they didn't create themselves, or misrepresent themselves as an author or creator of something found online. Research conducted via the Internet should be appropriately cited, giving credit to the original author.

Personal Safety

Students should never share personal information, including phone number, address, social security number, birthday, pictures, or financial information over the Internet without adult permission. Students should recognize that communicating over the Internet brings anonymity and associated risks, and should carefully safeguard the personal information of themselves and others. Users should never agree to meet someone they meet online in real life without parental permission.

If students see a message, comment, image, or anything else online that makes them concerned for their personal safety, they should bring it to the attention of an adult (teacher or staff at school; parent at home) immediately.

STUDENT USE OF TECHNOLOGY (continued)

Cyberbullying

Cyber bullying will not be tolerated. Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyber stalking are all examples of cyber bullying. Students should not be mean, 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, cyber bullying can be a crime. Students should remember that their activities are monitored and retained.

If students see a message, comment, image, or anything else online that looks or feels like bullying, they should bring it to the attention of an adult (teacher or staff at school; parent at home) immediately.

Terms of Agreement

- I will use school technologies for school-related activities.
- I will follow the same guidelines for respectful, responsible behavior online that I am expected to follow offline.
- I will not damage, change, or tamper with the hardware, software, settings or the network in any way.
- I will not seek, view, send, or display offensive messages or media.
- I will obey copyright laws and properly cite sources when using online resources.
- I will not share my passwords with another person
- I will not harm other people or their work.
- I will not trespass in another's folders, work, or files.
- I will not interfere with the operation of the network.
- I will not use my personal email account or any personal electronic device at school except with the permission of a staff member.
- I will notify an adult immediately if by accident I encounter materials which violate the rules of appropriate use.

STUDENT USE OF TECHNOLOGY (continued)

- I will not use any form of electronic communication to harass, intimidate, or bully anyone.

- I am prepared to be held accountable for my actions and for the loss of privileges if these rules are violated.

Web 2.0 Terms of Agreement

- I will act safely by keeping personal information out of my Web projects. I will not give out my family name, email address, home address, schools name, city, country or other information that could help someone locate or contact me in person. I will not post identifying photos or videos.

- I will treat blog and wiki spaces as I would a classroom space, and I will use appropriate and respectful language and images.

- If I post a link in a blog, podcast, videocast or wiki, I will have read that information carefully to be certain that it is appropriate for the school community.

- I understand that if I fail to follow these guidelines, I may lose the opportunity to take part in the project.

- This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

Limitation of Liability

McCabe Union Elementary School District will not be responsible for damage or harm to persons, files, data, or hardware. While McCabe Union Elementary School District employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness. McCabe Union Elementary School District will not be responsible, financially or otherwise, for unauthorized transactions conducted over the school network, for copyright violations, or any harm or damages resulting from user mistakes or negligence, or from the willful violation of this agreement.

Violations of this Acceptable Use Policy

Violations of this policy may have disciplinary repercussions, including:

- Suspension of network, technology, or computer privileges

- Notification to parents

STUDENT USE OF TECHNOLOGY (continued)

- Detention or suspension from school and school-related activities
- Legal action and/or prosecution

I have read, I understand, and I agree to abide by the McCabe Union Elementary School District's Acceptable Use of Technology Agreement. I understand Violations may result in my loss of the network and/or Internet access, loss of technology, use, disciplinary action and possible legal action. I will sign my name to show that I will follow these rules.

Please sign and return the signature page for the Acceptable Use of Technology Agreement for Students Grades K-8 in Parent Packet #2.