Student Use of the Internet and Electronic Communications

All users of the Brush School District computer systems by either students or employees are subject to this Acceptable Use Policy (AUP). This bulletin will undergo periodic review to ensure District data systems are used in a responsible, efficient, ethical, and legal manner, and such use must be in support of the District's business and education objectives.

Teachers, administrators, and other school personnel should ensure District data systems are used in a responsible, efficient, ethical, and legal manner, and such use must be in support of the District's business and education objectives.

Philosophy of use
Access to computers, computing equipment, e-mail and the Internet enables students to explore thousands of libraries, databases, and Web sites while exchanging messages with Internet users throughout the world. The district provides students with computing and Internet access to further educational goals and objectives. However, students may find ways to access materials that are illegal, defamatory, inaccurate, or potentially offensive to some people. The district believes the benefits of access to the Internet in the form of information resources and opportunities for collaboration exceed any disadvantages.

Nevertheless, Brush School District RE2 (J) supports and respects each family's right to decide whether to apply for student access to the district's computer network.

Student rights and responsibilities for using the district network
The district provides a computer network for students who agree to act in a considerate and responsible manner. The network is available to conduct research, save student work and files, and communicate with others via email.

Access is a privilege, not a right, and therefore, entails responsibility. Students are responsible for good behavior on school computer networks just as they are in a classroom or school hallway. All users will comply with all district regulations and will honor signed agreements. Students and parents shall be required to sign the Brush School District RE 2(J) Acceptable Use Policy annually before Internet or electronic communicating accounts shall be accessed and be allowed.

Personal Internet use, Students' home use, and personal Internet use can have an impact on the school and on other students. If a student's personal Internet expression - such as a threatening message to another student or a violent Web site – creates a likelihood of material disruption of the school's operations, the student may face school discipline and criminal penalties.

Teacher supervision
During the instructional day, teachers make reasonable efforts to supervise student use of the district's Internet system in a manner that is appropriate to the student's age and circumstances of use.

Outside of school, families bear the responsibility for guiding their students in the use of the Internet much as they exercise guidance over television, telephones, movies, radio, and other potentially offensive media.

Student IDs and passwords
The district may provide any student with a unique Internet ID and password for that student's use only. All secondary students will receive an email account and elementary students by request for Teacher lead projects. The Technology Department will be available to consultation and assistance in efforts to incorporate technology into planned curriculum.

Students shall not share their passwords with anyone else, nor shall students use anyone else's password, regardless of how the password is obtained. Students who suspect that someone has discovered their password should contact the Technology Specialist at their school immediately. Students shall not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users.

Protection of identifying information
When sending electronic messages on the district's network or to users outside the network, students shall not include information that identifies themselves or other students. Identifying information includes, but is not limited to, last names, addresses, telephone numbers, family information, or any other personal information that could be used inappropriately. Students shall not arrange face-to-face meetings with persons met on the Internet or through electronic communications.

Students shall identify themselves by first names only.

Using proxy sites to by-pass district filters
Any use of school systems to bypass the established proxy server will result in disciplinary action that can include complete loss of computer privileges, suspension and/or expulsion.

Access to restricted use and physical computer damage
Student use of school district computer equipment and network is limited to the educational purposes specifically authorized by the student's teacher or instructor. Improper uses include, but are not limited to, gaining illegal access to school district records, files, computer programs, student records, and other information maintained by the school district; and using, altering, or damaging computers or computer data maintained by third parties, including members of other computer networks accessible through the school district's network.

Students shall not damage district or outside computing systems or networks or interfere with another's ability to use a computing system or network by releasing viruses, worms, e-mail bombs, or any other programs that slow, stop, or damage applications, computing systems, or networks.

Use of non-district software and applications
Students shall not install any non-district approved application software on the district network or school workstations. Any non-district thumb-drive/memory stick/flash drive, USB drive must be

scanned for computer viruses by in-school Technology specialists before students may use them in district computers.

Students may **NOT** download inappropriate Internet files onto district network drives, into home directories, or onto workstation hard drives unless the student first obtains written permission from the Brush School District RE2(J) Technology. Inappropriate Internet files include, but are not limited to, games, music, video or audio files, or material protected by the district's filtering or blocking software.

Filtering software
In compliance with the Children's Internet Protection Act (CIPA), the district has installed filtering and/or blocking software to restrict access to Internet sites containing material harmful to minors, such as sexually explicit or other inappropriate materials. The software works by scanning for objectionable words or concepts as determined by the school district.
However, no software is foolproof. A user who incidentally connects to an inappropriate site must immediately disconnect from the site and notify a teacher or supervisor. If a user sees another user accessing inappropriate sites, he or she should notify a teacher or supervisor immediately.

Students shall not tamper with the filtering service. Such tampering will result in loss of computer privileges for no less than one quarter.

Students shall not use the school district's network system to access material that is obscene, pornographic, sexually explicit, sexually suggestive, harmful, or otherwise inappropriate.

Personal expression
The following restrictions against inappropriate speech and messages apply to all speech communicated and accessed through the district Internet system, including e-mail, instant messages, Web pages, and Web logs.

Students shall not send obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful messages. Students shall not post information that could cause damage, danger, or disruption, or engage in personal attacks, including prejudicial or discriminatory attacks. Students shall not harass another person, or knowingly or recklessly post false or defamatory information about a person or organization.

Cyber bullying
Brush School District RE2(J) does not tolerate bullying and harassment by computer.
Students shall not use any Internet or other communication device, such as cell or telephone to intimidate, bully, harass, or embarrass other students or staff members. Students who engage in such activity on school grounds or who engage in such activity off campus and create material disruption of school operations shall be subject to the penalties outlined in the Student Conduct Code as well as possible criminal prosecution.

Prohibited activities
As outlined by policy and district regulations on student rights and responsibilities, the following activities are prohibited on the district's network, Internet, and wireless access systems:

- Sending, displaying, or printing offensive messages, materials, photos, or pictures that are intended to stimulate erotic feelings, exhibit nudity, or sexual jokes or acts.
- Using obscene language
- Harassing, insulting, or attacking others
- Discriminating or defaming others based on religion, race, color, creed or sexual orientation.
- Sending threatening, inflammatory, or violent communications
- Offering for sale, purchase, or use of any prohibited or illegal substances
- Damaging computers, computer systems, computer networks, or wireless systems
- Downloading games, MP3, or music based files
- Playing Internet-based games or activities or participating in text-based or audio based chats
- Violating copyright laws
- Using another's password
- Using another student ID as the student's own
- Using a teacher ID as the student's own
- Theft identity of another individual's login/ID or password
- Trespassing in another user's folders, work, or files
- Using technology, computers, scanners, or other peripherals to produce counterfeit reproductions
- Buying or selling on E-bay or similar auction sites
- Displaying and/or printing instructions for making weapons, accessing anything that promotes violence or advocates destruction of property, or conducting illegal activities, i.e., Anarchist Handbook
- Intentionally wasting resources
- Employing the network for commercial purposes, including, but not limited to, posting advertisements to a news group, using e-mail to solicit sales, or using Web sites to advertise or sell a service
- Damaging, destroying, or deleting software or the work of another individual or group
- Any other activity inconsistent with the stated intent of this computer network or wireless agreement

Student safeguards:

Web publishing
Students who publish Web sites on the district's network must adhere to district policy regarding student safety:

- Web documents shall include only first names or initials of students
- Web documents shall not include student home telephone numbers or addresses nor the names or any personal information regarding family members or friends
- Web documents on the Brush School District Internet servers shall not include student e-mail addresses

- No Web documents may feature an individual student without that student's signed Acceptable Use Policy parental release form, with the exception of previously published references
- Students who publish first names or photographs of other district students are responsible for ensuring that those students have a signed Acceptable Use form and have given written permission for publishing said information.

Policy parental release form

- Parents who sign the Acceptable Use Policy form are providing permission to publish their students' Web pages
- Web documents shall not be used to solicit sales, conduct business, advertise, or sell a service

Copyright infringement

Students shall not:

1. Copy and forward; copy and download; or copy and upload to the district network or Internet server any copyrighted material without the approval of the computer system operator, a teacher, or other school administrator.

Copyrighted material is defined as anything written by someone else. Examples include an e-mail message, a game, a story, an encyclopedia entry, or software. Students shall use proper methods to cite Internet sources on reports and documentation, including any text, images, and graphics downloaded from the Internet.

District Access to Student Files and Emails

Students should have no expectation of privacy or confidentiality in the content of electronic communications or other computer files that they send or receive on the school computer network or store in student directories.

The Director Technology or other District employee may, at any time, review the subject, content, and appropriateness of electronic communications or other computer files and may remove them, if warranted. The Director of Technology or other District employee will report any violation of state or federal law or of district policy or regulation to the school administration or law enforcement officials.

Cell phones, iPODS, Blackberries, and Other Technology

Students may bring cell phones, iPODS, Blackberries, and other communication devices to school as long as they do not disrupt the educational process. Individual schools and teachers may impose additional restrictions.

The district is not responsible for the loss, theft, damage, or vandalism to student cell phones or other student electronic devices.

Policy on Sexting

It is an explicit part of this policy that a student may not possess, view, send, or share pictures or text having sexual content while the student is on school grounds, at school sponsored events or

on school buses or other vehicles provided by Brush Schools. This policy strictly prohibits sexual material in electronic or any other form and includes but is not limited to the sexual material contained in a cellular telephone, camera phone, or personal digital assistant and sexual material transmitted by text message, e-mail, or any electronic communication device. A student who violates this policy is subject to suspension or expulsion.

It is also a violation of Colorado criminal statutes to possess, create, photograph, exhibit, or disseminate certain categories of material of a sexual nature that meet the definitions of child exploitation or child pornography. School personnel are required to report to law enforcement or child protective services whenever there is reason to believe that any student or other person in involved with child exploitation or child pornography. A person who is convicted of child exploitation or adjudicated a juvenile delinquent for violating the child exploitation statute is required to register with the State of Colorado as a sex offender.

Students and parents need to be aware of the consequences - some of them life-altering - of having sexual material at school, including on your cell phone or other electronic communication device.

Discipline
Brush School District may apply discipline up to and including suspension and/or expulsion for specific student violations of the Internet and Electronic Mail Permission and Use Regulations. Students who violate the Internet-use rules set forth in this regulation will be subject to the penalties established in the Code of Student Conduct.
Students are expected to review the Code of Student Conduct before using school computers or the district network. In addition, violations also may result in:

- Immediate removal from the computer network at any time without warning.
- Removal from the computer network for a specified period of time as determined by the principal, if the violation is limited to one computer and/or is contained in the school building.
- Removal from the computer network for a specified period of time as determined jointly by the principal in consultation with the Director of Technology and the other district staff, if the violation significantly threatens or damages district wide network resources, i.e., Web site, e-mail network, online grading system, etc.
- Permanent removal from the computer network for the duration of a student's enrollment in the district as determined by district administration.

District retains right to terminate access
Brush School District technology staff may terminate a user's network access and this agreement at any time without warning.

Unauthorized computer or network use subject to prosecution
Students who engage in unauthorized computer or network use may be subject to imprisonment, fines, and civil liability under applicable state and federal laws, including the Computer Fraud and Abuse Act (18 U.S.C.§ 1030), the Electronic Communications Privacy Act (18 U.S.C.§ 2510-2520 and 18 U.S.C § 2701-2710), and C.R.S. § 18-5.5- 101.102. Unauthorized computer or network use

may also result in disciplinary measures consistent with the school district's policies and regulations, including suspension and expulsion.

Nothing herein shall be deemed to prevent a teacher or instructor from establishing additional rules and conditions, subject to the ultimate control of the district administration and the Board of Education.

I have read, understand, and agree to abide by the provisions of the Acceptable Use Policy of the Brush School District.

Date: _____/_____/_____

School: _____

Student Name: _____

Student Signature: _____

Parent/Legal Guardian Name: _____

Parent/Legal Guardian Signature: _____

Please return this form to the school where it will be kept on file. It is required for all students that will be using a computer network and/or Internet access.

Brush School District

Acceptable Use Policy (AUP) for District Computer Systems

Information for Employees

This Acceptable Use Policy was adopted by the Board May 2010

The District's Acceptable Use Policy ("AUP") is to prevent unauthorized access and other unlawful activities by users online, prevent unauthorized disclosure of or access to sensitive information, and to comply with the Children's Internet
Protection Act ("CIPA"). As used in this policy, "user" includes anyone using the computers, Internet, email, chat rooms and other forms of direct electronic communications or equipment provided by the District (the "network."). Only current students or employees are authorized to use the network.

The District will use technology protection measures to block or filter, to the extent practicable, access of visual depictions that are obscene, pornographic, and harmful to minors over the network. The District reserves the right to monitor users' online activities and to access, review, copy, and store or delete any electronic communication or files and disclose them to others as it deems necessary. Users should have no expectation of privacy regarding their use of District property, network and/or Internet access or files, including email.

Acceptable Uses of the Brush Computer Network or the Internet
Access is provided primarily for education and District business. Staff may use the Internet, for incidental personal use during duty-free time. By using the network, users have agreed to this policy. If a user is uncertain about whether a particular use is acceptable or appropriate, he or she should consult a supervisor or other appropriate District personnel.

Unacceptable Uses of the Computer Network or Internet
These are examples of inappropriate activity on the District web site, but the District reserves the right to take immediate action regarding activities (1) that create security and/or safety issues for the District, students, employees, schools, network or computer resources, or (2) that expend District resources on content the District in its sole discretion determines lacks legitimate educational content/purpose, or (3) other activities as determined by District as inappropriate.

• Violating any state or federal law or municipal ordinance, such as: Accessing or transmitting pornography of any kind, obscene depictions, and harmful materials, materials that encourage others to violate the law, confidential information or copyrighted materials;

• Criminal activities that can be punished under law;

• Selling or purchasing illegal items or substances;

• Obtaining and/or using anonymous email sites; spamming; sexting; spreading viruses;

• Causing harm to others or damage to their property, such as:

1. Using profane, abusive, or impolite language; threatening, harassing, or making damaging or false statements about others or accessing, transmitting, or downloading offensive, harassing, or disparaging materials;
2. Deleting, copying, modifying, or forging other users' names, emails, files, or data; disguising one's identity, impersonating other users, or sending anonymous email;
3. Damaging computer equipment, files, data or the network in any way, including intentionally accessing, transmitting or downloading computer viruses or other harmful files or programs, or disrupting any computer system performance;
4. Using any District computer to pursue "hacking," internal or external to the District, or attempting to access information protected by privacy laws; or
5. Accessing, transmitting or downloading large files, including "chain letters" or any type of "pyramid schemes.

• Engaging in uses that jeopardize access or lead to unauthorized access into others' accounts or other computer networks, such as:

1. Using another's account password(s) or identifier(s);
2. Interfering with other users' ability to access their account(s); or
3. Disclosing anyone's password to others or allowing them to use another's account(s).

• Using the network or Internet for Commercial purposes:

1. Using the Internet for personal financial gain;
2. Using the Internet for personal advertising, promotion, or financial gain; or
3. Conducting for-profit business activities and/or engaging in non-government related fundraising or public relations activities such as solicitation for religious purposes, lobbying for personal political purposes.

Student Internet Safety

1. Students shall not reveal on the Internet personal information about themselves or other persons. For example, students should not reveal their name, home address, telephone number, or display photographs of themselves or others;
2. Students shall not meet in person anyone they have met only on the Internet; and
3. Students must abide by all laws, this Acceptable Use Policy and all District security policies.

Penalties for Improper Use

The use of a District account is a privilege, not a right, and misuse will result in the restriction or cancellation of the account. Misuse may also lead to disciplinary and/or legal action for both students and employees, including suspension, expulsion, dismissal from District employment, or criminal prosecution by government authorities. The District will attempt to tailor any disciplinary action to the specific issues related to each violation.

Disclaimer

The District makes no guarantees about the quality of the services provided and is not responsible for any claims, losses, damages, costs, or other obligations arising from use of the network or accounts. Any additional charges a user accrues due to the use of the District's network are to be borne by the user. The District also denies any responsibility for the accuracy or quality of the information obtained through user access. Any statement, accessible on the computer network or the Internet, is understood to be the author's individual point of view and not that of the District, its affiliates, or employees.

Adopted: June 15, 2010