Policy FY2012-AUP, - Technology Acceptable Use Policy

1. Purpose

The purpose of this policy is to ensure appropriate, responsible, ethical and legal access and use of computers, the Internet, and other electronic or communication devices by District students, patrons, and employees. The Technology Acceptable Use Policy AUP addresses two distinct concepts of technology use. The first regards the use of computers and the Internet, and the second addresses interfering and electronic communication devices.

As the district moves towards the student:computer ratio of 1:1, policy and protocol changes are expected to address the philosophy of the school and the technology infrastructure.

2. Policy

2.1. Computers and the Internet

It is the policy of the Beaver County School District to permit students, patrons, and employees to have computer and Internet access under approved regulations and guidelines, to include those listed in the Children's Internet Protection Act, State Law, and policies adopted by Board (of Education). In general, the user's responsibilities require responsible, decent, ethical, polite, efficient, and legal use of computer and network resources. Students, patrons, and employees must not access obscene, pornographic, or material that is deemed to be harmful to minors. District and school personnel will instruct students and staff on acceptable use of computers and Internet resources and proper network etiquette. All students, patrons, and employees are granted access to the Internet, but all access to the Internet through district resources is subject to the terms of the Technology Acceptable Use Agreement and District policy.

2.2. Interfering and Electronic Communication Devices

While in some instances the possession and use of electronic communication devices or other devices or objects by a student at a school may be appropriate, often the possession and use of such devices or objects by students at school can have the effect of distracting, disrupting, and intimidating others in the school setting and leading to opportunities for academic dishonesty and other disruptions of the educational process. The purpose of this component of the policy is to vest with school administrators the authority to enforce reasonable rules relating to student use of such objects or devices in the public schools. School level procedures may be enacted in addition to those found in district policies and this AUP.

3. Procedure

3.1. Definitions:

3.1.1. **Acceptable Use**: Computer and Internet use must be consistent with the education objectives of the District. The use must also be consistent with the terms of this agreement.

3.1.2. **Prohibited Use**: Any use that violates federal or State laws and/or District policy.

3.1.3. **Interfering Devic**e: This includes any device or object which does not constitute a weapon or explosive but may, if used or engaged, interfere with the educational

process for either the student possessing or using the object or for other students. By example, such objects include any electronic communication device (defined below), a camera, lasers, laser pens or pointers, radios, portable CD players, or other electronic equipment or devices.

3.1.4. **Electronic Communication Devic**e: This includes laptop and hand-held computers, telephones, “smart phones”, camera telephones, two-way radios or video broadcasting devices, pagers, and any other device that allows a person to record and/or transmit on either a real time or delayed basis, sound, video or still images, text, or other information.

3.1.5. **Camera:** This includes any device for taking still or motion pictures, whether in a digital or other format.

3.1.6. **CIPA** – Child Internet Protection Act - CIPA, provides for educating minors about appropriate online behavior. This certification, which includes the appropriate online behavior for interacting with other individuals on social networking websites and in chat rooms and cyber-bullying awareness will be taught to all students in Beaver County School District in age appropriate settings.

3.1.7. **BYOD** - A general term that deals with individuals *“bringing their own devices”* and connecting them to the district network via WiFi.

3.1.8. **NetSafeUtah** - The NetSafe Utah project includes presentations, workshops and online resources for kids, teens, parents and educators. NetSafe Utah is adapted continually to provide Utah schools and communities the Internet Safety information they need and helps schools meet Children’s Internet Protection Act (CIPA) requirements.

3.2. Prohibited Uses: The following uses of the District's computers, including its network and Internet access are prohibited for:

3.2.1. Using an account other than your own and any attempt to gain unauthorized access to accounts on the network within or outside the district.

3.2.2. Attempting to obtain access to restricted sites, servers, files, databases, etc. Attempts to gain unauthorized access to other systems (e.g. "hacking").

3.2.3. Student use of games, Internet games, chat rooms, blogs, social networking sites, non-district sponsored or approved email services, and instant messaging not specifically assigned or authorized for use by a teacher or an administrator. Employees, students and patrons must not use games, gambling/gaming sites, Internet games, chat rooms, blogs, social networking sites, non-district sponsored or approved email services, and instant messaging that is not directly related to curriculum development, instruction, or work assignment. If such sites are blocked, access can be requested for appropriate, core-aligned uses. Exceptions could include teacher controlled classroom activities.

3.2.4. Using computers, the Internet or network for any illegal activity. This includes, but is not limited to: gambling, copyrighted material, sensitive, libelous, injurious, threatening or obscene material, bullying, pornography or material protected by trade

secrets. This prohibition includes the violation of any federal, State or local law, district or school policy or procedure..

3.2.5. Providing personal addresses, phone numbers, and other private information whether that information belongs to the user or any other individual unless it is related to the core curriculum or specifically authorized for release. Additionally, all employees are subject to and must comply with State and federal privacy laws and regulations. The unauthorized disclosure of private or protected information may result in disciplinary action and referral for criminal prosecution.

3.2.6. Using the Internet for commercial purposes, financial gain, personal business, product advertisement, use for religious or political lobbying (including student body elections students or union/association representation elections for employees)

3.2.7. Attempting vandalism defined as any attempt to harm or destroy data of another user, another agency or network that is connected to the Internet. Vandalism includes, but is not limited to, the uploading, downloading, or creation of computer viruses. It also includes attempts to gain unauthorized access to a network that is connected to the Internet.

3.2.8. Degrading or disrupting network equipment, software, or system performance.

3.2.9. Wasting finite network resources.

3.2.10. Invading the privacy of individuals or disclosing confidential information about other individuals.

3.2.11. Posting personal communications without the original author's consent.

3.2.12. Posting anonymous messages.

3.2.13. Accessing, downloading, storing, forwarding or printing files or messages that are profane, obscene, or that use language that offends or tends to degrade others.

3.2.14. Harassing others or using abusive or obscene language on the network. The network may not be used to harass, bully, annoy, or otherwise offend other people.

3.2.15. Using material which may be deemed to violate any District policy or student code of conduct.

3.2.16. Downloading music or video files or any other files that will infringe on copyright laws or is not directly related to a school or position assignment.

3.2.17. Communicating threats of violence.

3.2.18. Using the network for plagiarism. Plagiarism is taking ideas or writing from another person and offering them as your word. Credit must always be given to the person who created the information or idea.

3.2.19. Bypassing district filters and security via proxy servers, VPN access, or other means.

3.2.20. Unauthorized purchasing of goods or services online. The District is not responsible for any such purchases. Goods or services may not be purchased using district computers services that are not acceptable or legal in the public school system. .ie. firearms, alcohol, tobacco, controlled substances, pornographic materials, etc..

3.2.21. using VoIP (Voice over IP) software or devices not endorsed by the district.

3.2.22. installation and use of personal wireless access points. All wireless network access (if any) will be provided by the District.

3.3. Privileges and Discipline:

Internet use is a privilege, not a right, and inappropriate use will result in a loss of network privileges, disciplinary action, and/or referral to legal authorities. The system administrators will close an account when necessary. An administrator or faculty member may request the system administrator to deny, revoke, or suspend specific user access and/or user accounts. District employees, to include teachers, staff, and administrators, may face disciplinary action up to and including termination. Authorized District employees have the right to intercept or read a user's e-mail, to review any material, and to edit or remove any material that they believe may be unlawful, obscene, defamatory, abusive or otherwise objectionable. There is no expectation of privacy on any district owned or controlled computer, storage device, email service, electronic or analog file. If the District intends to impose any discipline upon a student other than revoking privileges for the remainder of the school year, the student will be afforded appropriate or adequate due process. Career and Provisional Employees will be disciplined according to District Policy. Temporary employees or other patrons may be denied computer access or have their employment terminated.

3.4. Privacy Information:

Nothing is private on the District-owned network. If a user accesses a particular site on the Internet, it is likely that someone knows the connections that the user is making, knows about the computer the user is using and what the user looked at while on the system. Frequently these sites maintain records that can be subpoenaed to identify what the user has been viewing and downloading on the Internet. In addition, the District reserves the right to monitor whatever a user does on the network and to make sure the network functions properly. A user has no expectation of privacy as to his or her communications or the uses made of the Internet or any district computer services while on school time or using school facilities or equipment.

3.5. Network Etiquette:

Users are expected to abide by the generally accepted rules of network etiquette. These include but are not limited to the following:

- be polite.
- do not be abusive in your messages to others.
- use appropriate language.
- do not swear, use vulgarities or any other language inappropriate in a school setting.

3.6. Security:

3.6.1. Security is a high priority on computer networks. If a security problem is identified, the user must notify the system administrator immediately. Do not demonstrate the

problem to other users. Users may not use the Internet to discuss or disseminate information regarding security problems or how to gain unauthorized access to sites, servers, files, etc.

3.6.2. Any passwords issued to users/parents/guardians must not be shared with or disclosed to other users without specific authorization from the administrator. Passwords should be changed frequently. If students/parents divulge passwords to anyone not authorized by school policy, the school/district cannot guarantee the protection of confidential student information.

3.6.3. Do not leave a workstation without logging out of the network or "locking down" the workstation.

3.6.4. You must report any of the following to a building administrator:

- if you receive or obtain information to which you are not entitled;
- if you know of any inappropriate use of the network by others; and
- if you believe the filtering software is not filtering a site or sites that should be filtered under this agreement.

3.7. Disclaimer:

3.7.1. The District makes no guarantee of the completeness or accuracy of any information provided on the network. It makes no promise or warranty to maintain or update its network or the information contained or made available to the public, its employees, and students. The District may suspend or discontinue these services at anytime. The user assumes the risk of verifying any materials used or relied on.

3.7.2. The District disclaims any express or implied warranty in providing its computer system, provided services and any materials, information, graphics, or processes contained therein. It makes no warranty, express or implied, nor assumes any responsibility regarding the use of its network or its contents for its accuracy, completeness, currency, its use of any general or particular purpose, or that such items or use of such items would not violate or infringe on the rights of others. Access to its network is provided on a strictly "as is basis."

3.7.3. The District's network resources may contain hypertext or other links to Internet or computer sites not owned or controlled by the District that may be of interest. The District cannot supervise or control the content of these other sites. Any information, endorsements of products or services, materials or personal opinions appearing on such external sites are not controlled, sponsored or approved by the District.

3.7.4. The District specifically disavows legal responsibility for what a user may find on another external site or for personal opinions of individuals posted on any site, whether or not operated by the District.

3.7.5. A user assumes the risk of use or reliance on any information obtained through the network.

3.7.6. The District will not be responsible for any damages a user suffers while on the system, including loss of data resulting from delays, non-deliveries, mis-deliveries or service interruptions caused by negligence, errors, or omissions.

3.8. Access and/or Accounts Requirements

All users are responsible for reading and agreeing to follow all guidelines outlined in the Acceptable Use Agreement (AUA). Employees may be granted an account for their term of employment subject to the terms, limitations, and conditions outlined in this policy.

3.9. Interfering and Communication Devices

Except as set forth below, a student may possess, but may not operate or engage, any interfering device during school hours or at school functions, unless specifically authorized in advance by the school personnel in charge of the class or activity.

3.9.1. It is District policy that students and others in the District will not be subject to video or audio capture, recording or transmission of their words or images by any student at a school without express prior notice and explicit consent for the capture, recording or transmission of such words or images.

3.9.2. During any time when a student is scheduled to be in class or involved in a regular school activity, it is a violation of policy for the student to have in his or her possession an electronic communication device or camera which is in the "on" position and ready to receive, send, capture, or record any communication, visual image, sound, text message or other information.

3.9.3. Electronic communication devices and cameras must not be possessed, activated, or utilized at any time by any person, to include a student, teacher, staff employee, patron, or any other individual, in any school situation where a reasonable expectation of personal privacy exists. These locations and circumstances include but are not limited to locker rooms, shower rooms, restrooms, and any other areas where students or others may change or be in any stage or degree of disrobing or changing clothes.

3.9.4. The principal or administrator of the school is hereby given authority to make determinations as to other specific locations and situations where possession of electronic communication devices and cameras is absolutely prohibited.

3.9.5. At no time may any electronic communication device or camera be utilized by any student in any way which gives the impression to others of being threatened, humiliated, harassed, embarrassed, or intimidated.

3.9.6. A school may possess a security system that utilizes cameras for the express purpose of recording both video and audio of events within the school. The building administrator is responsible for the security of these systems and confidentiality associated with this recorded media. This media will be used for identity, prosecution, and establishing timelines. Security equipment should not be located where a reasonable expectation of personal privacy exists.

3.10. Sanctions Confiscation of Device

Any electronic device found on District property is subject to search and confiscation. Pornographic or indecent material will be reported for possible criminal prosecution in accordance with the UCA 76-10-1235 and/or other applicable District, state and federal regulations. For each observed violation of this policy, it shall be the duty of the school staff,

teacher or administrator observing the violation to immediately confiscate the interfering device. Employee or patron violations will be immediately reported to the appropriate school or District administrator. Furthermore, the school or District may take additional disciplinary action as described in other District policies. The confiscated device shall be forwarded to the administrative office together with the name of the person from whom the device was confiscated and the reason for the confiscation. The school office should make arrangements to notify the parent/guardian of the student from whom the device was confiscated and arrange for the parent or guardian to pick up that device at the school office. Any concern with suspected violations of a person's safety, privacy, rights or due process will immediately be forwarded to the school's uniformed resource officer for criminal investigation. Violations may also warrant an internal investigation by the school district for possible expulsion.

3.11. Employee Disciplinary Actions shall be in accordance with applicable laws, regulations and District policies.

3.11.1 Disciplinary actions will follow existing board policy. Obvious criminal violations will be investigated by both the Sheriff's Office and the District Administration.

3.12. Student Disciplinary Actions:

3.12.1. Any use of an electronic communication device or camera to record sounds or images or otherwise capture material in an unauthorized setting or at an unauthorized time shall subject the user of the device to increased discipline based on the circumstances and whether the student has been involved in prior violations of this policy and/or other District Policies.

3.12.2. The use of any interfering device or any electronic communications device or camera to threaten, intimidate, or embarrass another or to capture and transmit test information or any other information in a manner constituting fraud, theft, or academic dishonesty may result in an immediate suspension of not less than three days nor more than ten days.

3.12.3. The use of any interfering device in a manner which may be physically harmful to another person, such as shining a laser in the eyes of another student, may result in an immediate suspension of not less than three days nor more than 10 days. When a student repeatedly engages in such behavior, the punishment may be increased as is appropriate. Authority: 53A-3-402(15) 53A-11-901 et seq. Utah Code Annotated

3.13. CIPA, ERTE Form 479, Internet Safety Protection:

3.13.1. CIPA requires schools and libraries that seek E-rate discounts for Internet access and internal connections to certify that they have in place certain Internet safety policies and technology protection measures.

3.13.2. All district school principals (Appendix B) will certify that on a yearly basis, all students in their school were present for at least two events concerning NetSafeUtah where internet safety, cyber bullying, bullying of any type, online predators, and educational instruction on accepted internet practices are discussed and questions are allowed to be addressed.

3.13.3. All district training will utilize and incorporate materials from the Utah Education Network's Net Safe Utah project. Animated materials will be used for grades K-6 while 7-12 materials address increased awareness situations such as: Cyber bullying,

Appropriate Uses of Technology, Cell Phone Safety, Internet and Violence Addiction, Being a Good Digital Citizen, Acceptable Internet Behaviors and Social Networking. Educational Materials for educating minors on appropriate access can be found at: http://www.netsafeutah.org/educators/training/index.html

3.13.5. The district's Internet safety policy provides for the education of minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyber-bullying awareness and response".

Policy FY2012-1 Telecommunication Devices

1. Purpose

Use of wireless communication devices and cellular phones in particular has become increasingly prevalent with high school and elementary school students in addition to staff. These devices offer tremendous convenience and access to communication with parents and other students. With such convenience and ease comes the great potential for misuse and abuse of this technology.

2. Policy

While in some instances the possession and use of wireless communication devices or other devices or objects by a student at a school may be appropriate, often the possession and use of such devices or objects by students at school can have the effect of distracting, disrupting, and intimidating others in the school setting and leading to opportunities for academic dishonesty and other disruptions of the educational process. The purpose of this policy is to vest with school administrators the authority to enforce reasonable rules relating to student use of such objects or devices in the public schools.

3. Procedure

3.1. Definitions:

3.1.1a. **Acceptable Student Use**: Students are not permitted to use any type of wireless communication device during class time, passing periods or breaks without the permission of the school administration. The wireless communication device must remain turned off and out of sight during the instructional school day. Some instructors may allow students to use these devices in class, but the use must not disrupt the learning environment and will conform to the policies set forth. This policy does not disallow the use of polling devices when sanctioned by the classroom teacher.

3.1.1b. **Acceptable Staff Use**: Staff members are permitted to use any type of wireless communication device during class time, passing periods or breaks provided the use is acceptable per building policy. The wireless communication device may remain on and in silent mode during the instructional school day. Under no condition can the device disrupt the learning environment and must conform to the policies set forth.

3.1.2. **Prohibited Use**: Any use that violates federal or State laws and/or District policy.

3.1.3. **Electronic wireless communication devic**e: This includes laptop and hand-held computers, telephones, “smart phones”, camera telephones, two-way radios or video broadcasting devices, pagers, and any other device that allows a person to record and/or transmit on either a real time or delayed basis, sound, video or still images, text, or other information. School issued equipment may be exempt from certain expectations.

3.2. Prohibited Uses: Students and staff are not to use material, images or text message to invade personal privacy or harass another person, or disrupt the instructional day, or engage in dishonest acts. The following are inappropriate uses of electronic wireless communication devices:

3.2.1. Harassment, threats, intimidation, cyberbullying/cyberthreats of other students, teachers, staff or school administration via cellular phone calls, SMS text messaging or by the use of MMS picture messaging.

3.2.2 Passing or transmitting otherwise secure information, i.e. electronic forgery.

3.2.3 Invasion of personal rights in any school situation where a reasonable expectation of personal privacy exists. These locations and circumstances include but are not limited to locker rooms, shower rooms, restrooms, and any other areas where students or others may change or be in any stage or degree of disrobing or changing clothes.

3.2.4 Cheating on tests/exams by either transmitting or receiving test/exam information or images before, during, or after the administration of the test/exam.

3.2.5 Violation of any other district policy or other forms of illegal behavior during the instructional and non- instructional day.

3.2.6 School Bus Operators or staff members transporting students on a school approved activity: It is the school bus operator's responsibility, in accordance with policy and training instructions, to keep his/her attention and awareness on the safe operation of the school bus, the safety of all passengers, and the safety of the public at all times.

3.2.7 School Bus Operators or staff members transporting students on a school approved activity: A school bus operator shall not wear a cell phone, blue tooth, or other wired or wireless device while the school bus is in motion and not stopped and appropriately secured. This includes devices such as headsets, earpieces, earphones, or any other equipment that might distract a driver from their responsibilities.

3.2.8 School Bus Operators or staff members transporting students on a school approved activity: If the bus is stopped and appropriately secured, a bus driver may use these devices for emergencies, for special needs students, behavior management, field/activity trips, or other district or school business related issues.

3.2.9 School Bus Operators or staff members transporting students on a school approved activity: A driver may use these devices for personal use once the bus is safely parked, appropriately secured off the roadway and all passengers are safely off and moved away from the bus.

3.3. Privileges and Discipline:

3.3.1 Students are allowed to use their wireless communication devices before school, during their designated lunchtime, and after school in accordance with the above policies.

3.3.2 Students may have the cell phones in their possession or in their lockers at other times during the instructional day as long as the device is turned off and powered down and the device is out of sight in a pocket, bag or backpack.

3.3.3 If a student receives permission by a teacher or school administration to use a wireless communication device, it shall not disrupt the educational program.

3.3.4 If disruption occurs, the school staff shall direct the student to turn off the device and/or confiscate it.

3.3.5 If a school staff member finds it necessary to confiscate a device, parents will be notified promptly and the device will be returned in accordance with school rules after the administrator or designee has consulted with the student's parent/guardian.

3.3.6 The school is not responsible for lost or stolen electronic wireless communication devices. Students are to make arrangements with their parent(s) or guardian(s) to contact the school office when attempting to reach them during the school day.

3.3.7 Staff member violations will be dealt with by their immediate supervisor.

3.3.8 Students who act in violation of this policy shall be subject to the District's progressive discipline as follows:

1. Initial violation – wireless communication device will be confiscated by school staff and secured in a safe location under the principal's direction. The device will be returned to student at the conclusion of the school day;
2. Second violation – wireless communication device will be confiscated and secured in a safe location under the principal's direction. The device will not be returned to the student until the student's parent or guardian contacts the school administrative staff for the purpose of clarifying this policy;
3. Third violation – the wireless communication device will be confiscated and secured in a safe location under the principal's direction. The device will not be returned to the student until the student's parent or guardian provides written assurance that the student will no longer be allowed to possess the device during the instructional day.
4. Fourth violation – the wireless communication device will be confiscated and secured in a safe location under the principal's direction. The student will be subject to suspension;
5. Fifth violation – the wireless communication device will be confiscated and secured in a safe location under the principal's direction. The student will be subjected to loss of school privileges;
6. Any further violations will subject the student to further disciplinary action.

Individual schools may enact their own time line and requirements for items 1-6.

Policy FY2012-2

Wireless Connecting to the District Infrastructure

1. Purpose

This policy establishes standards that must be met when wireless communications equipment is connected to Beaver County School District networks. The policy prohibits access to Beaver County School District networks via unsecured wireless communication mechanisms.

2. Scope

This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, Bluetooth equipped devices, and 802.15 devices etc.) connected to any of Beaver County School District's internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to Beaver County School District's networks do not fall under the purview of this policy.

3. Policy

3.1 Approved equipment

All wireless LAN access must use district-approved products and security configurations. All network equipment, both wired and wireless, must be purchased & installed by District technology personnel. Schools are not permitted in any way of using or procuring any access device that connects to the district network unless endorsed by the district.

3.2 Monitoring of uncontrolled wireless devices

All District locations where permanent data networks are installed may be equipped with sensors and systems to automatically detect, classify, and disrupt communication with unapproved (rogue) wireless access points. All District locations where permanent data networks are installed may be equipped with sensors and systems to automatically detect the presence of wireless devices forming a connection between the network and any wireless network. This would include laptops that are serving as a bridge between wired and wireless networks or computers participating in ad-hoc or peer-to-peer wireless networking. In District locations where wireless LAN access has been deployed, whenever possible, wireless intrusion detection systems may be deployed to monitor for attacks against the wireless network.

3.3 Authentication of wireless clients

All access to wireless networks must be authenticated. The District's existing strong password policy must be followed for access to wireless networks. The strongest form of wireless authentication permitted by the client device must be used. Violations of the configured rules, indicating that an intrusion has taken place, must cause the device to be immediately disconnected and blocked from the network. Any District user with an account in a District user database may be able to authenticate at any District location where wireless access is present.

The current expectation for "strong password" security is as follows: an acceptable password for use on district computer services is expected to contain 8 total characters with at least 3

alpha characters, 2 numeric characters and an other character. Examples of strong passwords would be ajbr#345 or aBel$45a. Both upper and lower case characters are recommended.

3.4 Encryption

All wireless communication between District devices and District networks must be encrypted. Wireless networks providing only Internet access for guest users are exempted from this requirement. The strongest form of wireless encryption permitted by the client device must be used. Violations of the configured rules, indicating that an intrusion has taken place, must cause the device to be immediately disconnected and blocked from the network.

3.5 Access control policies

- Access to District network resources through wireless networks should be restricted based on the role of the user.
- Unnecessary protocols should be blocked, as should access to portions of the network with which the user has no need to communicate.
- Access control enforcement shall be based on the user's authenticated identity, rather than a generic IP address block. This is also known as "identity-based security." The access control system must be implemented in such a way that a malicious inside user is unable to bypass or circumvent access control rules.
- Access control rules must use stateful packet inspection as the underlying technology.

3.6 Remote wireless access

Telecommuting employees working from remote locations must be provided with the same wireless standards supported in District offices. Employees should be discouraged from connecting District computers though consumer type wireless equipment while at home in lieu of District-provided equipment. Remote users outside of the district network must connect to district resources using a secure connection such as a VPN.

3.7 Client security standards

- All wireless clients are expected to run District approved anti-virus software that has been updated and maintained in accordance with the District's anti-virus software policy.
- All wireless clients must run host-based firewall software in accordance with the District's host security policy.
- All wireless clients must have security-related operating system patches applied that have been deemed "critical" in accordance with the District's host security policy.
- All wireless clients must be installed with District-standard wireless driver software. Clients not conforming with minimum security standards will be placed into a quarantine condition and automatically remediated. Client operating systems that do not support client integrity checking will be given restricted access to the network according to district requirements.

3.8 Wireless guest access

- Wireless guest access may be available at all facilities where wireless access has been deployed for guest use.
- All wireless guest access will be authenticated through a web-based authentication system (captured portal).
- A single username/password combination will be assigned for all guest access. The password for guest access will be changed monthly and distributed to local facility managers. Special accounts

may be created for guests on a request basis. Access must be arranged at least 24 hours before planned access.

- Wireless guest access bandwidth may be limited.
- Guest access may be restricted to the following network protocols:

    - HTTP (TCP port 80)
    - HTTPS (TCP port 443)
    - IMAP (TCP 143)
    - POP (TCP port 110)
    - IKE (UDP port 500)
    - IPSEC ESP (IP protocol UDP 50)
    - PPTP (TCP port 1723)
    - GRE (IP protocol 47)
    - DHCP (UDP ports 67-68)
    - DNS (UDP port 53)
    - ICMP (IP protocol 1)

Policy FY2012-3 User Passwords

1. Purpose

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the District's entire school network. As such, all District employees (including contractors and vendors with access to the District's systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2. Policy

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change. The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any District facility, has access to the District network, or stores any non-public District information.

3. Procedure

3.1. General:

3.1.1. All admin-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.

3.1.2 All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months.

3.1.3 User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.

3.1.4 Passwords must not be inserted into email messages or other forms of electronic communication.

3.1.5 All user-level and system-level passwords must conform to the guidelines described below.

3.2. Guidelines:

3.2.1 General Password Construction Guidelines

Passwords are used for various purposes in our District. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight (8) characters

- The password does not contain any non-alphabetic characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
- Names of family, pets, friends, co-workers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware, software.
- The words "Beaver County School District", "<School Name>", "<City>" or any derivation.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight (8) alphanumeric characters long and is a passphrase (Ohmy1stubbedmyt0e).
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

3.2.2. Password Protection Standards

3.2.2.1 Do not use the same password for District accounts as for other non-District access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various District access needs. For example, select one password for the Grading and Student Information systems and a separate password for Web and Email systems. Also, select a separate password to be used for an NT account and a UNIX account.

3.2.2.2 Do not share District passwords with anyone, including administrative assistants or secretaries.

3.2.2.3 All passwords are to be treated as sensitive, confidential District information.

3.2.2.4 Here is a list of "dont's":

• Don't reveal a password over the phone to ANYONE unless a known identity is established

• Don’t allow others to access your computer or the District computer systems using your password

• Don’t share any private passwords with students

- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

3.2.2.5 If someone demands a password, refer them to this document or have them call someone in the Information Security Department.

3.2.2.6 Do not use the "Remember Password" feature of applications (e.g., Outlook, Internet Explorer, Firefox, Messenger).

3.2.2.7 Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

3.2.2.8 Change passwords at least once every six months (except system-level passwords which must be changed

quarterly). The recommended change interval is every four months.

3.2.2.9 If an account or password is suspected to have been compromised, report the incident to the District Technology Director and change all passwords.

3.2.3 Passphrases

Passphrases are generally used for public/private key authentication. Without the passphrase to "unlock" the private key, the user cannot gain access. Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

Policy FY2012-4

Computer Anti-Virus Protection – Software Installation

1. Purpose

This policy establishes standards and best practices that must be met when any computer or computing device, both wired and wireless, is connected to Beaver County School District networks to prevent obtaining and spreading computer viruses. These are basic steps that all users must take to ensure that Beaver County School District computers and networks remain stable and available at all times.

2. Scope

This policy covers all users of computers running any sort of user installable and configurable operating systems (Windows, Mac OS, Linux, etc.) that are used in the District or are connected to the District network either through a wired Ethernet connection or by wireless networking.

3. Policy

3.1 Expectations

3.1.1 Users are expected to use district installed and approved software applications only.

3.1.2 Users are not authorized to install unlicensed software on computers. If a user requires special or non-standard software to be installed on computers for District use, it must be cleared by District Technology. The user will be responsible for supplying licenses, media, and any documentation. License information is a requirement of the District Auditors. Only district licensed software will be installed by District staff. School level purchases will be installed by the school level tech.

3.1.3 Users are ultimately responsible for their own data. Users must back up critical data and system configurations on a regular basis and store the data in a safe place.

3.1.4 Users must run the District standard, supported anti-virus software that is available from the District Technology Director or his designees. Users must run the current version and download and install anti-virus software updates as they become available.

3.1.5 Any district machine found with non district approved or installed software, must have the original copy of the license present and to remain with the computer for the duration of its installation. Trial software packages are discouraged and may only remain on district computers for the time of the trial at which time they must be removed. Computers found with unsubstantiated software will be re-imaged by district when found.

3.1.6 Any unlicensed software installed on an assigned computer will be the responsibility of the assigned user and their immediate supervisor(bldg administrator).

3.2 Best Practices

3.2.1 Never open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.

3.2.2 Delete spam, chain, and other junk email without forwarding, in accordance with the Districts Acceptable Use Policy.

3.2.3 Never download files from unknown or suspicious sources.

3.2.4 Avoid direct disk sharing with read/write access unless there is absolutely a District requirement to do so.

3.2.5 Always scan a floppy diskette or any portable storage device from an unknown source for viruses before using it.

3.2.6 New viruses are discovered almost every day. Periodically check the Anti-Virus for updates and download and install any available updates.

3.2.7 Always use the current & up to date version of any software application on your computer. The District will not attempt to make old or outdated software work with newer installed operating systems.

3.3 Results of Non-Compliance

3.3.1 Any non-approved software installations will not be supported.

3.3.2 Any machine that is found to have software installed that has not been approved by the district or does not have a current and active license will be reformatted and all data will be wiped clean. In addition, any software piracy issues become the problem of the installer and not District Computer Services. Anyone installing software that violates any portion of licensing or acceptable use become the problem of the installer.

3.3.3 Any machine that has been infected by a virus that can not be removed from a Users computer will be formatted and wiped clean of all data. The District will reinstall the appropriate system operating software and District approved software only. Any user data on the machine may/will be lost.

Policy FY2012-5

Publishing on the Internet

1. Purpose:

District websites provide instructional resources; information about curriculum, instruction and school authorized activities; and general information relating to our schools and our District's mission. Communication with parents, family, the community and students is important for the District and each classroom teacher. Events and projects can be displayed to show what has been happening in the classroom along with keeping all informed about future events and assignments. It is important that teachers give their web page address to students and parents as often as possible and keep their site updated.

Beaver County School District teachers will be allowed to create and post their own web pages to the Internet. This will place the primary responsibility for the content of the teacher's page on the teacher. Building administrators and the Beaver County School District are also responsible under federal law for the content of these pages. Teachers should be extremely careful whatever they post. It is the responsibility of the teacher, the building administrators and the District to ensure that all District hosted web pages follow District policies and state and federal laws. This guide is intended to assist District personnel and teachers in the development and posting of web pages.

2. Policy:

2.1. Teachers posting web pages on District sponsored web servers must adhere to the established rules and guidelines.

2.2. Posting of student work on District sponsored web servers must be in compliance with the established rules and guidelines.

3. Procedure:

3.1. Web Page Rules and Guidelines

3.1.1. This policy provides the basic overview for teachers posting web pages linked to the District webpage. Among the key points are:

3.1.1.1. Teachers and administrators are encouraged to develop links to third party hosts. The links need to conform to the "three-click rule" so that the link does not provide connection to inappropriate sites.

3.1.1.2. Teachers and administrators need to attend training sessions if they are going to create and maintain a District web site.

3.1.1.3. The District encourages teachers to involve students in the development of web sites. (Involvement needs to be grade appropriate. Students can be involved in various aspects including layout, design, choosing colors, and offering suggestions).

3.1.1.4. All web pages are subject to evaluation at any time by District administrators.

3.1.1.5. School administrators are responsible for evaluating the content on the school's website, its teacher's pages, and any links off of these pages.

3.1.2. The content and links within the District, school, or teacher web site should:

3.1.2.1. be informative.

3.1.2.2. be accurate.

3.1.2.3. be current.

3.1.2.4. pertain to education or to the functions of the school.

3.1.2.5. be correctly written, spelled and punctuated.

3.1.2.6. be thoughtfully and attractively presented.

3.1.2.7. have written parental permission to display a student's name or picture. Although student names and photos are considered "directory information," written parental permission must be obtained because of the potential worldwide dissemination and loss of control of this information.

3.1.2.8. insure that a student CANNOT be identified by attaching his/her name to a specific picture, phone number or address.

3.1.2.9. have written permission in order to display the name or picture of any staff member or School Board member.

3.1.2.10. require written permission be obtained for single, specific pictures or it may be generally given for District approved use.

3.1.2.11. allow adults to be identified by attaching his/her name to a specific picture, phone number or address with written permission.

3.1.3. Content and links (defined as any site that can be reached in two clicks or less) within the District web site or, a teacher/student page linked from the District site, should NOT:

3.1.3.1. contain or point to pornographic, violent, obscene, objectionable or offensive material.

3.1.3.2. violate copyright laws by containing unauthorized or plagiarized content including but not limited to written materials, pictures, graphics, audio, and video.

3.1.3.3. contain any personal information on students without written parental permission.

3.1.4. In order to protect individual privacy and promote good community relations, District web sites or, teacher/student pages linked from the District website, should:

3.1.4.1. never provide addresses, phone numbers or other private information about students.

3.1.4.2. never post individual pictures with the student's first or last names.

3.1.4.3. only post class pictures that include three (3) or more students and do not include information explaining the positioning of individuals in the picture.

3.1.4.4. never provide e-mail addresses except for the purpose of supporting or providing feedback for a school-related activity, organization or web site.

3.1.4.5. never contain information or material that the District would not be willing to publish in other media forms (e.g., newspaper, television, brochures, etc.).

3.1.4.6. never allow students to post their personal web pages. If students need to post a web page as part of integrating the classroom curriculum with the Internet, it should be posted on the District web page with teacher approval through the District web master. All links from a student project web page must be checked for appropriateness.

3.1.4.7. never promote specific political, metaphysical or religious viewpoints or agendas. Links to such pages may be placed on a web page for research purposes if the links are balanced.

3.2. Internet Release Form

3.2.1. The release form must be signed by teachers, administrators, staff and other individuals to give permission for information to be placed on a web page hosted by the District or any of the District's schools. Guest speakers and other special event participants that will be featured on the web page should also sign this form.

It is the responsibility of the web page creator/teacher to ensure the release form is signed and maintained if any of the following are posted on a web page:

1. First Name
2. Photograph
3. Published Project (If an individual's project is to be published on a teacher's web page, it is the responsibility of the teacher to ensure that all copyright issues are addressed.
4. Email Address

Policy FY2012-6

BYOD – Bring Your Own Device

1. Purpose

BCSD believes that student learning processes seem to be accelerated when students incorporate all avenues available to complement the learning process. Privately owned devices were once thought to be incompatible with the district technology infrastructure. While every effort was made to block student devices from entering school campuses, incorporating their presence now seems to be not only acceptable but encouraged. In addition, personal devices connected to the building infrastructure also helps the schools approach the 1:1 device per student solution.

On March 1, 2011, BCSD began allowing students to use privately owned electronic devices to access the BCSD wireless network at all district property locations. This wireless access provided to the devices is designed to enhance the students' educational experience and outcomes. Connecting to the BCSD Wi-Fi network with personal devices is a privilege, not a right, and *it is not a requirement* for students. Permission to bring and use privately owned devices is contingent upon adherence to BCSD guidelines. If a privately owned device is used by a student to disrupt the educational environment, in the sole opinion of BCSD, that student's privileges may be limited or revoked.

2. Scope

This policy pertains specifically to non-district owned personal devices. Students/Patrons/Employees should understand that the specific expectations of this and other district technology policies are interwoven to provide a stable environment for a progressive use of technology.

3. Policy

3.1 Expectations

- 3.1.1 All students may use a privately owned electronic "Internet ready" device on the BCSD wireless network by completing and submitting the attached BYOD Policy Agreement to his/her homeroom teacher.
- 3.1.2 The use of the privately owned electronic device is solely limited to support and enhance instructional activities currently occurring in the classroom environment.
- 3.1.3 Recognizing that all such devices may not be appropriate for instructional situations, personal electronic devices will be considered for classroom use if they are mobile and have the capability of browsing the Internet. These items include, but are not limited to: laptops, netbooks, tablets, cell phones, e-readers and hand-held gaming devices. The final determination of devices that are appropriate to connect to the BCSD network rests with the District IT.Students are prohibited from accessing the internet using private 3G or 4G subscriptions through their own Internet Service Provider.
- 3.1.4 Connecting a privately owned electronic device may not be successful if the technical specifications for wireless protocol are not met. Devices must use 802.11g or 802.11n Wi-Fi connectivity only to access the division's wireless network.
- 3.1.5 No privately owned electronic device may be attached to any BCSD network if a signed AUP and BYOD policy form are not on file in the BCSD student information system.
- 3.1.6 All information related to the privately owned electronic device(s) that is requested by this form will be submitted by the student prior to accessing the network.
- 3.1.7 No student shall establish a wireless ad-hoc or peer-to-peer network using his/her electronic device or any other wireless device while on school grounds. This includes, but is not limited to using a privately owned electronic device as a cabled or wireless hotspot. Example: Using a personal device as a server so that students can play an online game; e.g. Battlefield Heroes, Warflow. The student may not provide ISP type connections to other students for the purpose of allowing another device to connect to the internet via a private account or connection.

3.1.8 No privately owned electronic device should ever be connected by cable to the BCSD network. Network access is provided via Wi-Fi / wireless connection only. No one is allowed to connect a privately owned electronic device to the network by an Ethernet cable plugged into a data jack in the school. Violation of this term will result in disciplinary action and revocation of access to the network.

3.1.9 Teacher permission is necessary for student use of a privately owned electronic device during classroom instruction or the classroom period.

3.1.10 Voice, video, and image capture applications may only be used with prior written teacher permission and for specific instructional purpose(s).

3.1.11 The teacher may request at any time that the privately owned electronic device be turned off and put away. Failure to do so may result in disciplinary action and revocation of access to the network.

3.1.12 Sound should be muted unless the teacher grants permission for use of sound associated with the instructional activities.

3.1.13 The privately owned electronic device owner is the only person allowed to use the device.

3.1.14 No student shall use another student's district-issued log-on credentials.

3.1.15 No student shall knowingly attempt to gain access to any computer, computer system, computer network, information storage media, or peripheral equipment without the consent of authorized school or division personnel.

3.1.16 No district-owned academic or productivity software can be installed on personal devices.

3.1.17 Under no condition will any form of BULLYING be allowed using an electronic device connected through the district network.

3.1.18 No student shall use any computer or device to illegally collect any electronic data or disrupt networking services. Students may not engage in any malicious use, disruption or harm to the school network, Internet services, learning environment or any other electronic device owned by the school, any school personnel and/or student.

3.1.19 Students may not attempt to use any software, utilities or other means to access Internet sites or content blocked by school division internet filters.

3.1.20 Under the provisions of the BYOD program, parents who choose to allow students to use their own technology and students who bring personal technology do so knowing that it will diminish their expectation of privacy regarding their personal electronic device while at school. The school reserves the right to search a privately owned electronic device in accordance with applicable laws and policies if there is reasonable suspicion that the student has violated BCSD policies, administrative procedures, school rules, or engaged in other misconduct while using the device.

3.1.21 Devices are brought to school at the students' and parents' own risk. In the unlikely event that a privately owned device is lost, stolen or damaged, BCSD is not responsible for any financial or data loss.

3.2 Best Practices

3.2.1 CIPA, SafeSchools, and other protective instruction for our students proctection should be taught in classroom curriculum on a regular basis.

3.2.2 Laptops and other portable electronic devices are vulnerable to loss and theft. These devices should be engraved or otherwise permanently marked with owner information. Students and parents who choose to allow their children to bring privately owned electronic devices on school property must assume total responsibility for these devices and be aware of all risks. If a privately owned electronic device is stolen, this must be reported to a building administrator immediately. BCSD will not accept responsibility for loss, damage or theft of personal property.

3.2.3 Never access sites that are unknown or suspicious.

3.2.4 Laptops and all other personal electronic devices that are lost, stolen, or damaged are the responsibility of the student and their parents or guardians. School district and school personnel cannot attempt to repair, correct, troubleshoot, or be responsible for malfunctioning personal hardware or software.

3.2.5 Do not let others use your personal device to send texts, messages, emails, etc.

3.2.6 New viruses are discovered almost every day. Please equip your private devise with acceptable virus protection.

3.3 Results of Non-Compliance

3.3.1 Violation of school or division policies, local, state and/or federal laws while using a personal electronic device on the BCSD wireless network will result in appropriate disciplinary and/or legal action as specified in the Student AUP, school rules/protocols, School Board policy as well as by local, state and/or federal law.

3.3.2 Any devise that has been infected by a virus will be removed from the network.

Policy FY2012-7

Student/Faculty/Staff Email Accounts

1. Purpose

Effective communication and the benefits of cloud storage, cloud tools and devices have increased the need for all students and staff to have access to some type of cloud based storage, tool box, secure and easily accessible suite of internet based tools. BCSD has currently chosen to utilize the GOOGLE GMAIL platform as the sole provider for our district.

Using this cloud based tool chest, all users will have access to word processing, spreadsheet and presentation software. In addition, cloud storage and a variety of other tools will be provided aslo.

2. Scope

By utilizing Google Tools and the Gmail platform, all students and staff will have uninterrupted access at home and school to their file storage and their tools to produce, edit and finalize.

3. Policy

3.1 Expectations

3.1.1 All district staff and students from Grades 4-12 will have a Gmail account created for them.

3.1.2 Users will be preloaded with accounts names based on district standards and passwords that may be a series of characters identifiable with student record similarities.

3.1.3 Students are expected to use the accounts to store, edit, and forward their work based on the needed scenario.

3.1.4 Users must adhere to District standards and rule as listed in the current AUP.

3.1.5 The student email account and tool access account will remain the same through out the student's career.

3.1.6 All email account remain the property of Beaver County School District and can be searched at any time for reason.

3.2 Best Practices

3.2.1 Only store materials that a needed for your successful educational path.

3.2.2 Delete junk email without forwarding, in accordance with the Districts Acceptable Use Policy.

3.2.3 Never download files from unknown or suspicious sources.

3.2.4 Never use district owned equipment to download any files from an unknown origin or containing any form of material that violates the current AUP.

3.3 Results of Non-Compliance

3.3.1 Anyone producing/opening/forwarding or advancing any type of email that attacks, demeans, causes any form of disruption, spams, interrupts, etc. will be deemed as an attack on computer services and will immediately be delt with based on the current AUP.

3.3.2 The cloud package of tools associated with the email account assigned to the user is a great advance to forward education in the district. Students should utilize all process for the advance of education. Any non-adherence to the AUP will be dealt with immediately.

Student Information Web Release Form

Student's Full Name: _____

I Authorize Beaver County School District and/or _____school to publish the following Information on the District's World Wide Web:

I **PERMIT** Beaver County School District and/or the school to publish:	I **DO NOT PERMIT** Beaver County School District or the school to publish:
My student's first name only My student's first & last name My student's photo My student's class work	My student's name My student's photo My student's class work

I understand that this information will be available to anyone on the World Wide Web.

Parent or Legal Guardian (*please print*):_____

Signature of Parent or Legal Guardian:_____

Date:_____

Please note that this does not replace the District's Acceptable Use Policy or imply permission to use Internet services. Publication of this data is not required to use Internet services.

Schools should keep the completed form on file at the school.

Student - Computer & Network Acceptable Use Policy

Please Note: When a student signs the Acceptable User Policy individually or in a handbook, it is also referring to this and other Board Approved and published District Policies; FY2012-AUP, FY2012-1, FY2012-2, FY2012-3, FY2012-4, FY2012-5, FY2012-6, FY2012-7. The Federal Law Appendix is located at the end of this document.

Please return this agreement, signed by student and parent, to your homeroom teacher.

Beaver County School District provides a wide array of technology resources for student use. This agreement, along with any student handbooks in each school, outlines appropriate use and prohibited activities when using technology resources. Every student is expected to follow all guidelines stated below, as well as those given orally by the faculty & staff, and to demonstrate good citizenship and ethical behavior at all times.

<u>In accepting this agreement, students acknowledge the following rules and conditions:</u>

As a Beaver County School District student, I understand that my school network and email accounts are owned and provided by the District and are not private. Beaver County School District has the right to access my information at any time.

GOVERNMENT LAWS:

I will use computers in conformity with laws, policies and procedures of the United States, the State of Utah, Beaver County School District and my school. Violations include, but are not limited to, the following:

1. Criminal Acts – These include, but are not limited to, “hacking” or attempting to access computer systems without authorization, harassing email, cyberstalking, child pornography, vandalism, theft, and/or unauthorized tampering with computer systems. (A list of Federal statutes from the United States Department of Justice is below as Appendix A).
2. Libel Laws - Publicly defaming people through the published material on the Internet, email, etc…
3. Copyright Violations - Copying, selling or distributing copyrighted material without the express written permission of the author or publisher (users should assume that all materials available on the Internet are protected by copyright), engaging in plagiarism (using other's words or ideas as your own).

NETIQUETTE and RESPONSIBLE USE:

1. I understand that passwords are private. I will not allow others to use my account name and password, or try to use that of others.
2. I will be polite and use appropriate language in my email messages, online postings, and other digital communications with others. I will not use profanity, vulgarities or any other inappropriate language as determined by school administrators.
3. I will use email and other means of communications (e.g. blogs, wikis, chat, instant-messaging, discussion boards, etc.) responsibly. I will not use computers, cell phones, personal digital devices or the Internet to send or post hate or harassing mail, make discriminatory or derogatory remarks about others, or engage in bullying, harassment, or other antisocial behaviors either at school or at home.
4. I understand that I am an Ambassador for the school in all my online activities. I understand that what I do on social networking websites such as MySpace and Facebook should not

reflect negatively on my fellow students, teachers, or on the District. I understand that I will be held responsible for how I represent my school and myself on the Internet.

5. I understand that masquerading, spoofing, or pretending to be someone else is forbidden and potentially illegal. This includes, but is not limited to, sending out e-mail, creating accounts, or posting messages or other online content (e.g. text, images, audio or video) in someone else's name as a joke.
6. I will use District computer resources responsibly. I will not retrieve, save, or display hate-based, offensive or sexually explicit material using any of the Districts computer resources. I am responsible for not pursuing material that could be considered offensive. I understand that I am to notify an adult immediately if by accident I encounter materials that violate appropriate use.
7. I will use district technology resources productively and responsibly for school-related purposes. I will not use any technology resource in such a way that would disrupt the activities of other users.
8. I will not attempt to bypass security settings or Internet filters, or interfere with the operation of the network by installing illegal software, shareware, or freeware on school computers.
9. I understand that vandalism is prohibited. This includes but is not limited to modifying or destroying equipment, programs, files, or settings on any computer or other technology resource.
10. I will respect the intellectual property of other users and information providers. I will obey copyright guidelines. I will not plagiarize or use other's work without proper citation and permission.
11. I will not use or access files, software, or other resources owned by others without the owner's permission. I will use only those District network directories that are designated for my use or for the purpose designated by my teacher.
12. I will follow all guidelines set forth by the District and/or my teachers when publishing schoolwork online (e.g. to a website, blog, wiki, discussion board, podcasting or video server).
13. I understand the Internet is a source for information that is both true and false; and that the school is not responsible for inaccurate information obtained from the Internet.
14. I understand that the District administrators will deem what conduct is inappropriate use if such conduct is not specified in this agreement.
15. I agree to abide by all Internet safety guidelines that are provided by the school and to complete all assignments related to Internet safety.
16. I understand that BCSD requires my participation in internet safety programs. I acknowledge that when these instructional courses present themselves that I will attend and adhere to the standards taught.

CONSEQUENCES FOR VIOLATION OF THIS AGREEMENT:

I understand and will abide by the above (AUP)Acceptable Use Agreement. Should I commit a violation, I understand that consequences of my actions could include suspension of computer privileges, school disciplinary action, and/or referral to law enforcement.

Student Signature: _____

Date _____

Parent or Guardian:

As the parent or guardian of this student, I have read the Acceptable Conduct and Use Agreement. I understand that computer access is provided for educational purposes in keeping with the academic goals of Beaver County School District, and that student use for any other purpose is inappropriate. I recognize it is impossible for Beaver County School District to restrict access to all controversial materials, and I will not hold the District responsible for materials acquired on the District network. I understand that children's computer activities at home should be supervised as they can affect the academic environment at school. I expect my student to abide by all policy set forth in FY2012-AUP of the district approved policies.

I hereby give permission for my child to use computer resources at Beaver County School District.

Parent or Guardian's Name (please print_____

Parent or Guardian's Signature _____

Date _____

Employee - Computer & Network Acceptable Use Policy

Please Note: When an employee signs the Acceptable User Policy individually or via their employment contract, it is also referring to this and other Board Approved and published District Policies; FY2012-AUP, FY2012-1, FY2012-2, FY2012-3, FY2012-4, FY2012-5, FY2012-6, FY2012-7.. The Federal Law Appendix is located at the end of this document.

Please return this signed agreement to your building administrator.

Beaver County School District provides a wide array of technology resources for staff use. This agreement, along with other district and school policies, outlines appropriate use and prohibited activities when using technology resources. Every employee is expected to follow all guidelines stated below, as well as those given by their supervisors, fellow workers, district and school policies and procedures. All employees are expected to demonstrate good citizenship and ethical behavior at all times.

<u>In accepting this agreement, employee acknowledge the following rules and conditions:</u>

As a Beaver County School District employee, I understand that my computer, network and email accounts are owned and provided by the District and are not private. Beaver County School District has the right to access my information at any time.

GOVERNMENT LAWS:

I will use computers in conformity with laws, policies and procedures of the United States, the State of Utah, Beaver County School District and my school. Violations include, but are not limited to, the following:

1. Criminal Acts – These include, but are not limited to, “hacking” or attempting to access computer systems without authorization, harassing email, cyberstalking, child pornography, vandalism, theft, and/or unauthorized tampering with computer systems. (A list of Federal statutes from the United States Department of Justice is below as Appendix A).
2. Libel Laws - Publicly defaming people through the published material on the Internet, email, etc…
3. Copyright Violations - Copying, selling or distributing copyrighted material without the express written permission of the author or publisher (users should assume that all materials available on the Internet are protected by copyright), engaging in plagiarism (using other's words or ideas as your own).

NETIQUETTE and RESPONSIBLE USE:

1. I understand that passwords are private. I will not allow others to use my account name and password, or try to use that of others.
2. I will be polite and use appropriate language in my email messages, online postings, and other digital communications with others. I will not use profanity, vulgarities or any other inappropriate language as determined by school administrators.
3. I will use email and other means of communications (e.g. blogs, wikis, chat, instant-messaging, discussion boards, etc.) responsibly. I will not use computers, cell phones, personal digital devices or the Internet to send or post hate or harassing mail, make discriminatory or derogatory remarks about others, or engage in bullying, harassment, or other antisocial behaviors either at school or at home.

4 I understand that I am an Ambassador for the school in all my online activities. I understand that what I do on social networking websites such as MySpace and Facebook should not reflect negatively on the District. I understand that I will be held responsible for how I represent my school and myself on the Internet.
5 I understand that masquerading, spoofing, or pretending to be someone else is forbidden and potentially illegal. This includes, but is not limited to, sending out e-mail, creating accounts, or posting messages or other online content (e.g. text, images, audio or video) in someone else's name as a joke.
6 I will use District computer resources responsibly. I will not retrieve, save, or display hate-based, offensive or sexually explicit material using any of the Districts computer resources. I am responsible for not pursuing material that could be considered offensive. I understand that I am to notify my supervisor immediately if by accident I encounter materials that violate appropriate use.
7 I will use District technology resources productively and responsibly for school-related purposes. I will not use any technology resource in such a way that would disrupt the activities of other users.
8 I will not attempt to bypass security settings or Internet filters, or interfere with the operation of the network by installing illegal software, shareware, or freeware on school computers.
9 I understand that vandalism is prohibited. This includes but is not limited to modifying or destroying equipment, programs, files, or settings on any computer or other technology resource.
10 I will respect the intellectual property of other users and information providers. I will obey copyright guidelines. I will not plagiarize or use other's work without proper citation and permission.
11 I will not use or access files, software, or other resources owned by others without the owner's permission. I will use only those District network directories that are designated for my use or for the purpose designated by my supervisor.
12 I will follow all guidelines set forth by the District and/or my supervisor when publishing materials online (e.g. to a website, blog, wiki, discussion board, podcasting or video server).
13 I understand the Internet is a source for information that is both true and false; and that the district is not responsible for inaccurate information obtained from the Internet.
14 I understand that the District administrators will deem what conduct is inappropriate use if such conduct is not specified in this agreement.

CONSEQUENCES FOR VIOLATION OF THIS AGREEMENT:

I understand and will abide by the above Acceptable Use Agreement. Should I commit a violation, I understand that consequences of my actions could include termination, disciplinary action, and/or referral to law enforcement.

Employee Signature: _____Date _____

Appendix A –

Unlawful Online Conduct and Applicable Federal Laws

The chart below details the type of unlawful online conduct, potentially applicable federal laws, and the section of the Department of Justice with subject-matter expertise. If the subject matter expert is not a section of the Department, but rather another agency, the entry will have an asterisk following its initials. In many cases, prosecutors may also consider whether the conduct at issue is a violation of 18 U.S.C. § 2 (aiding and abetting) or 18 U.S.C. § 371 (conspiracy).

Unlawful Conduct	***Applicable Federal Law***	***DOJ Section***
Denial of Service Attacks	(a)(5)(A) (transmission of program, information, code, or command, resulting in damage)	CCIPS
	18 U.S.C. § 1362 (interfering with government communication systems)	CCIPS
Use of Misleading Domain Name	18 U.S.C. § 2252B (using misleading domain name with intent to deceive a person into viewing obscene material or with intent to deceive a minor into viewing harmful material)	CEOS
Password Fraud	18 U.S.C. § 1030 (a)(6) (trafficking in computer passwords)	CCIPS
	18 U.S.C. § 1029 (access device fraud)	Fraud/CCIPS
	18 U.S.C. § 1343 (wire fraud)	Fraud
Obscenity	47 U.S.C. § 223 (a)(1)(A) (using telecommunications device to make, create, or solicit, and transmit any obscene comment, request, suggestion, proposal, image, or other communication)	CEOS
	18 U.S.C. § 1465 (using interactive computer service for purpose of sale or distribution of obscene material)	CEOS
Piracy and Intellectual Property Theft	17 U.S.C. §§ 1201-1205 (Digital Millennium Copyright Act)	CCIPS
	17 U.S.C. § 506 and 18 U.S.C. § 2319 (criminal copyright infringement)	CCIPS
	18 U.S.C. § 2319A (trafficking in recordings of live musical performances)	CCIPS
Electronic Threats	18 U.S.C. § 875 (transmitting communications containing threats of kidnap or bodily injury) (Hobbs Act)	CTS
	18 U.S.C. § 1951 (interfering with commerce by robbery, extortion, threats or violence) (Hobbs Act)	DSS
	47 U.S.C. § 223 (a)(1)(C) (anonymously using	CCIPS

	telecommunications device to threaten person who receives communication)	
Electronic Harassment	47 U.S.C. § 223 (a)(1)(C) (anonymously using telecommunications device to harass person who receives communication)	CCIPS
	47 U.S.C. § 223 (a)(1)(E) (repeatedly initiates communication with a telecommunication device solely to harass person who receives communication)	CCIPS

Unlawful Conduct	***Applicable Federal Law***	***DOJ Section***
Interception of Electronic Communications	18 U.S.C. § 2511 (intercepting electronic communications)	CCIPS
	18 U.S.C. § 2701 (accessing stored communications)	CCIPS
	18 U.S.C. § 1030 (a)(2) (accessing a computer and obtaining information)	CCIPS
Cyberstalking	18 U.S.C. § 2261A (using any facility of interstate or foreign commerce to engage in a course of conduct that places person in reasonable fear of death or serious bodily injury to person, person's spouse or immediate family) See also Electronic Harassment	DSS
Hate Crimes	Look to civil rights laws and penalty enhancements	Civil Rights
Libel/Slander	Look to civil laws	
Posting Personal Information on a Website (e.g., phone numbers, addresses)	This is not a violation of law, but could be a violation of District Web Publishing policies.	
Invasion of Privacy	*See Interception of Electronic Communications*	
Disclosure of Private Information	18 U.S.C. § 2511 (1)(c) (disclosing intercepted communications)	CCIPS
Spam	18 U.S.C. § 1037 (CAN-SPAM Act)	CCIPS
Spoofing Email Address	18 U.S.C. § 1037 (CAN-SPAM Act)	CCIPS

Appendix B – Principal's Assurance of Education on Acceptable internet Practices

The District's "Internet safety policy provides for the education of minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyber-bullying awareness and response".

TO: Superintendent of Schools
Beaver County School District
Box 31
Beaver, Utah 84713

School Year _____

Dear Superintendent,

Please assured that during this school year, multiple offerings of internet safety training occurred as listed below. I assure you and the Beaver County School Board that every student in every grade were educated using resources from NetSafe Utah in acceptable internet behavior.

Cyber Bullying, Appropriate Uses of Technology, Cell Phone Safety, Internet and Violence Addiction, Being a Good Digital Citizen, Acceptable Internet Behaviors and Social Networking were among the materials taught using grade level appropriate materials.

Please log the following dates and detail for materials covered this year.

Date(s)	Grades Level(s)	Materials

If you have questions concerning this statement of assurance, please feel free to contact me.

_____ _____ _____

Principal Date School