ACCESS TO NETWORKED INFORMATION
COMPUTER-ASSISTED INSTRUCTION INTERNET SAFETY

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

DISTRICT INTERNET AND E-MAIL RULES.

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

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

INTERNET SAFETY TRAINING

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

The network is provided for students to conduct research and communicate with others. Access to network services is given to students who agree to act in a considerate and responsible manner. Parental permission is required. Access is a privilege, not a right. Access entails responsibility. Individual users of the District computer networks are responsible for their behavior and

communications over those networks. It is presumed that users will comply with District standards and will honor the agreements they have signed. Beyond the clarification of such standards, the District is not responsible for restricting, monitoring, or controlling the communications of individuals using the network.

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

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

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

1. sending or displaying offensive messages or pictures;

2. using abusive, objectionable or obscene language;

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

4. harassing, insulting or attacking others;

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

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

7. user shall not use or attempt to discover another user's password nor shall user use or let others use another person's name, address, passwords, or files for any reason, except as may be necessary for legitimate communication purposes and with permission of the other person;

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

9. intentionally wasting limited resources;

10. employing the network for commercial purposes;

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

12. user shall not tamper with computers, networks, printers, or other associated equipment or software without the express permission of supervising staff;

13. user shall not write, produce, generate, copy, propagate or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any computer's memory, file system or software.

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

15. Disclose, use or disseminate personal identification information regarding students.

SUPERVISION AND MONITORING

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

1. Follow the process prompted by the District's filtering software

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

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

4. Appeal of the decision to grant or deny access to a web site may be made in writing to the Board of Education. Persons who wish to remain anonymous may mail an anonymous request for review to the Board of Education at the School District's Central Office, stating the web site that they would like to access and providing any additional detail the person wishes to disclose.

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

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

In the event that a District student or employee feels that a web site or web content that is available to District students through District Internet access is obscene, child pornography, or "harmful to minors" as defined by CIPA or material which is otherwise inappropriate for District students, the

process described above should be followed, except any decision to filter or block web content will be made within thirty (30) days.

PENALTY

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

CROSS REF: EHAA-1-R User Agreement and Parental Permission Form
EHAA-2-R Employee Acceptable Use Agreement

Adopted: February 10, 1998
Revised: December 11, 2012

USER AGREEMENT AND PARENTAL PERMISSION FORM

As a user of the Uinta County School District No. Four computer network, I hereby agree to comply with School District policy EHAA and the rules set forth therein pertaining to communication over the Internet in a reliable fashion while honoring all relevant laws and restrictions. I agree only to use the Internet for legitimate, educational purposes. I do hereby expressly consent to allow school district personnel, including teachers, aides and administrators, to access and review any computer files, e-mail transmissions, and other computer data and/or information received by or sent from the student named below in order to ensure that the school district computers are being used appropriately and solely for educational purposes.

_____ × _____

Date Student

As the parent or legal guardian of the student signing above, I grant permission for my son or daughter to access the network for computer services, such as electronic mail and the Internet. I understand that individuals and families may be held liable for violations. I understand that some materials on the Internet may contain items that are illegal, defamatory, inaccurate or potentially offensive to some people, and I accept responsibility for guidance of Internet use, including setting and conveying acceptable standards to my son or daughter to follow when selecting, sharing, or exploring information on this network. We do hereby release the School District, its Board of Trustees, staff, and agents, from any liability of any kind arising out of our son's or daughter's use of the computer/Internet system at the school.

We do hereby authorize school district personnel, including teachers, aides and administrators, to access and review any computer files, e-mail transmissions, and other computer data and/or information received by or sent from the student named above in order to ensure that the school district computers are being used appropriately and solely for educational purposes.

Parent consents to allow school to use Internet (Web site) operators to offer online programs for the benefit of students and the school system, such as for communication regarding homework, facilitating online testing and/or communication regarding grades. The school requires that the service provider assure the school that it has in place a procedure or security system to maintain the confidentiality of any personal information that the service provider could have access to. Because these services or programs will necessitate giving access to student personal information to the Internet or Web site operators that host or facilitate these programs, the school must represent that it has parental permission for this and your execution of this policy/handbook shall be considered permission.

_____ × _____

Date Parent/Guardian

_____ × _____

Date Parent/Guardian

Adopted: February 10, 1998
Revised: January 11, 2000
Revised: December 11, 2012

EMPLOYEE ACCEPTABLE USE AGREEMENT

With the spread of telecommunications throughout the modern work place, the Board recognizes that employees will shift the ways they share ideas, transmit information and contact others. As staff members are connected to the global community, their use of new tools and systems bring new responsibilities as well as opportunities.

The Board expects that all employees will learn to use electronic mail and telecommunications tools and apply them frequently in appropriate ways to the performance of tasks associated with their positions and assignments. Toward that end, the Board directs the Superintendent to provide staff with training in the proper and effective use of telecommunications and electronic mail.

Communication over networks should not be considered private. Network supervision and maintenance may require review and inspection of directories or messages. Messages may sometimes be diverted accidentally to a destination other than the one intended. Privacy in these communications is not guaranteed. The District reserves the right to access stored records in cases where there is reasonable cause to expect wrong-doing or misuse of the system. Courts have ruled that old messages may be subpoenaed, and network supervisors may examine communications in order to ascertain compliance with network guidelines for acceptable use.

The Board directs the Superintendent and building principals to specify those behaviors which are permitted and those which are not permitted, as well as appropriate procedures to guide employee use. In general, employees are expected to communicate in a professional manner consistent with state laws governing the behavior of school employees and with federal laws governing copyrights. Electronic mail and telecommunications are not to be utilized to share confidential information about students or other employees.

The Board encourages staff to make use of telecommunications to explore educational topics, conduct research and contact others in the educational world. The Board anticipates that the new systems will expedite the sharing of effective practices and lessons across the District and will help staff stay on the leading edge of practice by forming partnerships with others across the nation and around the world.

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

The network is provided for employees to conduct research and communicate with others. Independent access to network services is provided to employees who agree to act in a considerate and responsible manner. Access entails responsibility.

Individual users of the District computer networks are responsible for their behavior and communications over those networks. It is presumed that users will comply with District standards and will honor any or all agreements they have signed.

Network storage areas may be treated like staff work areas. Network administrators may review files and communications to maintain system integrity and insure that users are using the system responsibly. Users should not expect that files stored on District servers will always be private.

Activities which are prohibited for which disciplinary and/or legal action could be taken include, but are not limited to the following:

- sending or displaying offensive messages or pictures;
- using obscene language;
- harassing, insulting or attacking others;
- damaging computers, computer systems or computer networks;
- violating copyright laws;
- using another's password;
- trespassing in another's folders, work or files;
- intentionally wasting limited resources;
- employing the network for commercial purposes;
- any other actions which are offensive or harmful to individuals or the District.

SANCTIONS:

1. Violations may result in a loss of access.
2. Additional disciplinary action may be determined at the building level in line with existing practice regarding inappropriate language or behavior.
3. When applicable, law enforcement agencies may be involved.

Employee signature: Date:

× _____ _____

Accepted by: Date:

× _____ _____

Adopted: February 10, 1998