Technology Acceptable Use Policy
Southwest Area Technology Team Collaborative Draft 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 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.

2. Policy

2.1. Computers and the Internet

> It is the policy of the (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.

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 or act that violates federal or State laws and/or District policy.

3.1.3. **Interfering Device**: 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.

3.2. 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.

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, and instant messaging not specifically assigned or authorized for use by a teacher or an administrator. Employees and patrons must not use games, Internet games, chat rooms, blogs, social networking sites, 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.

3.2.4. using computers, the Internet or network for any illegal activity. This includes, but is not limited to: copyrighted material, threatening or obscene material or material protected by trade secrets. This prohibition includes the violation of any federal, State or local law.

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 personal financial gain, personal business and product advertisement, or personal use for religious or political lobbying (including student body elections students or representation elections for employees, Reference District Policy 1600)

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 valuable network resources.

3.2.10. invading the privacy of individuals or disclosing confidential information about other individuals, if the disclosure is not allowed by state or federal law or district policies.

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

3.2.12. posting anonymous messages.

3.2.13. accessing, downloading, storing 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 and using abusive or obscene language on the network. The network may not be used to harass, 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 or entity and representing them as your own work. 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. using non-authorized VoIP (Voice over IP) software or devices.

3.2.21. 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 may 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 of employment. 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. 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 1450. 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.

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 in accordance with the User Password Guidelines. 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 as soon as possible:

- 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, misdeliveries 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 Policy (AUP). 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 in writing 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 written 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 the student's 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 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 has 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 to give the impression of threatening, humiliating, harassing, embarrassing, or intimidating others.

3.10. Sanctions Confiscation of Device

Pornographic or indecent material in possession by a student or staff member will be reported for possible criminal prosecution in accordance with the UCA 76-10-1235 and/or other applicable District or state actions. For each observed violation of this policy, it shall be the duty of the school or district staff, teacher or administrator observing the violation to immediately confiscate the interfering device. Employee 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 in a timely manner.

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

3.11.1 Specific policy and signature sheets for other District policies which may include:

Cell phone policy
User Password Guidelines
Publishing on the Internet
Student Information Web Release Form
Anti-Virus Policy
Wireless Security Policy

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.

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. When a student repeatedly engages in such behavior, the punishment may be increased as appropriate. Authority: 53A-3-402(15) 53A-11-901 et seq. Utah Code Annotated