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 Southwest Educational Development Center (SEDC) patrons, and employees.

2. Policy

- 2.1. Computers and the Internet

It is the policy of Southwest Educational Development Center (SEDC) to permit SEDC 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, Family Educational Rights and Privacy Act (FERPA), and policies adopted by the SEDC Board. In general, the user's responsibilities require responsible, decent, ethical, polite, efficient, and legal use of computer and network resources. SEDC patrons and employees must not access obscene, pornographic, or material that is deemed to be harmful to minors. In the event that students have access to the SEDC network, SEDC personnel will instruct these students and other staff members on a regular basis in appropriate online behavior including online safety, interacting with other individuals on social networking websites and in chat rooms, and regarding cyber-bullying awareness and response. SEDC will provide a technology protection measure (e.g. Internet filtering software) to help protect against access by users of the SEDC network of visually depictions that are obscene, child pornography, or — with respect to use of computers with Internet access by minors — harmful to minors. All SEDC patrons and employees are granted access to the SEDC Internet resources, but all access to

the Internet through SEDC is subject to the terms of the Technology Acceptable Use Agreement and SEDC policy.

3. Procedure

3.1. Definitions:

- 3.1.1. Acceptable Use: Computer and Internet use must be consistent with the education objectives of SEDC.
- 3.1.2. Prohibited Use: Any use or act that violates federal or State laws and/or SEDC 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 person possessing or using the object or for other people at SEDC. By example, such objects include any electronic communication device (defined below), a camera, lasers, laser pens or pointers, radios, portable DVD players, or other electronic equipment or devices.
- 3.1.4. Electronic communication device: This includes laptops and hand-held computers, telephones, mobile phones, two-way radios or video broadcasting devices, 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 and or sound, whether in a digital or other format.

3.2. Prohibited Uses:

The following uses of SEDC 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. using SEDC 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.

- 3.2.4. 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 work activities 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.
- 3.2.5. any commercial use, product advertisement not related to SEDC purposes or activities or promotion of political candidates.
- 3.2.6. 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.
- 3.2.7. degrading or disrupting network equipment, software, or system performance.
- 3.2.8. wasting valuable network resources.
- 3.2.9. invading the privacy of individuals or disclosing confidential information about other individuals, if the disclosure is not allowed by state or federal law or SEDC policies.
- 3.2.10. posting personal communications without the original author's consent.
- 3.2.11. posting anonymous messages.
- 3.2.12. accessing, downloading, storing or printing files or messages that are pornographic, indecent, profane, obscene, or that use language that offends or tends to degrade others.
- 3.2.13. 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.
- 3.2.14. using material which may be deemed to violate any SEDC policy code of conduct.
- 3.2.15. downloading music or video files or any other files that will infringe on copyright laws.
- 3.2.16. communicating threats of violence.

- 3.2.17. 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.
- 3.2.18. bypassing SEDC filters and security via proxy servers, VPN access, or other means.
- 3.2.19. using non-authorized VoIP (Voice over IP) software or devices.
- 3.2.20. installation and use of personal wireless access points. All wireless network access (if any) will be provided by SEDC.
- 3.2.21 excessive non-work related computer use during work hours.

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 Director will close an account when necessary. An administrator or faculty member can deny, revoke, or suspend specific user access and/or user accounts. SEDC employees, to include teachers, staff, and administrators, may face disciplinary action up to and including termination of employment. Authorized SEDC 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. Career and Provisional Employees will be disciplined according to SEDC 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 SEDC-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, SEDC personnel will monitor the use of SEDC computers and devices on a regular basis to ensure appropriate use and to make sure the network functions properly. A user on the SEDC network 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:

o be polite.

o do not be abusive in your messages to others.

o use appropriate language.

o 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 Director 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 given in a secure manner. Passwords should be handled in accordance with the User Password Guidelines. If a user divulges passwords to anyone not authorized by policy, SEDC cannot guarantee the protection of confidential information.
- 3.6.3. Do not leave an electronic communication device without logging out of the device or "locking down" the device.

- 3.6.4. You must report any of the following to the Director 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.
- 3.6.5. SEDC Password Procedures
  - Passwords should be saved and stored in a password manager.
  - Prevent the use of repetitive or incremental passwords
  - All user-created passwords are at least 8 characters in length and all machine-generated passwords are at least 6 characters in length. Passphrases are preferred.
  - Passwords must not be inserted into email messages or other forms of electronic communication.
  - Use Two-factor authentication (2FA) when available.

3.7. Disclaimer:

- 3.7.1. SEDC 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 patrons. SEDC may suspend or discontinue these services at any time. The user assumes the risk of verifying any materials used or relied on.
- 3.7.2. SEDC 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. SEDC network resources may contain hypertext or other links to Internet or computer sites not owned or controlled by SEDC that may be of interest. SEDC 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 SEDC.

- 3.7.4. SEDC 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 SEDC.
- 3.7.5. A user assumes the risk of use or reliance on any information obtained through the network.
- 3.7.6. SEDC 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 user may possess, but may not operate or engage, any interfering device, unless specifically authorized in advance in writing by SEDC personnel in charge.

- 3.9.1. It is SEDC policy that SEDC personnel or users of the network will not be subject to video or audio capture, recording or transmission of their words or images by anyone without express prior notice and explicit written consent for the capture, recording or transmission of such words or images.
- 3.9.2. Electronic communication devices and cameras must not be activated or utilized at any time by any person, to include a staff employee, patron, or any other individual, in the SEDC office where a reasonable expectation of personal privacy exists.
- 3.9.3. The Director has authority to make determinations as to other specific locations and situations where possession of electronic communication devices and cameras is absolutely prohibited.

- 3.9.4. At no time may any electronic communication device or camera be utilized by anyone 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 SEDC patron or staff member will be reported for possible criminal prosecution in accordance with the UCA 76-10- 1235 and/or other applicable SEDC or state actions. For each observed violation of this policy, it shall be the duty of the SEDC staff observing the violation to immediately confiscate the interfering device. Employee violations will be immediately reported to the Director. Furthermore, the Director may take additional disciplinary action as described in other 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.

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