

# ANW Special Education Cooperative Interlocal No. 603

## Computer, Network and Internet Acceptable Use Policy

Today we are challenged by rapidly changing, ever complex technologies in a diverse, mobile, and highly competitive society. Our future success as a Nation will largely depend on our society's ability to learn high-technology skills for work and informed citizenship. With properly used technology such as computer networks and Internet, our staff can increase student achievement, motivation, and learning opportunities.

The use of ANW Special Education Cooperative Interlocal No. 603 (ANW) computers, networks, and Internet is a privilege, not a right. It is a general policy that all computers shall be used in a responsible, efficient, ethical, and legal manner.

ANW makes no warranties of any kind, expressed or implied, for the computers, networks, and/or Internet access it is providing. ANW will not be responsible for any damages, including, but not limited to, loss of data or from delays or interruptions in service. ANW will not be responsible for the accuracy, nature, or quality of information stored on ANW storage media such as diskettes, hard drives, or servers; nor for the accuracy, nature, or quality of information gathered through ANW-provided Internet access. ANW will not be responsible for personal property used to access ANW computers, networks or Internet.

ANW's computers, network and Internet accounts are educational tools owned and paid for by ANW. ANW has the right at any time and for any reason to review all data, files and other records and information on ANW computers, and the right to periodically monitor, audit or review computer, network, Internet and e-mail use, including the right to review all e-mail and other electronic messages. The use of authorization passwords by staff or students shall not be construed as creating a private communication medium, and all such passwords shall be divulged to ANW upon request. The use of unauthorized or undisclosed passwords is strictly prohibited.

Even though ANW may use technical means to limit Internet access, these limits do not provide a foolproof means for enforcing the provisions of this policy. Some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate, or potentially offensive to some people. Goods and services can be purchased over the Internet that could potentially result in unwanted financial obligations. ANW will not be responsible for unauthorized financial obligations incurred by staff resulting from ANW-provided access to the Internet. Any such financial obligations are the sole responsibility of the staff member. Staff who utilizing ANW-provided computers, networks and Internet are responsible for good behavior on-line and in "electronic" field trips just as they are in a classroom or other area of the school.

GD Computer, Network and Internet Acceptable Use Policy

With the privilege of using the ANW computers, networks, and Internet come certain responsibilities. Staff members must familiarize themselves with these policies. Failure to follow these policies will result in disciplinary action.

1. Use of e-mail by students is prohibited;
2. Profanity, obscenity, and abusive, sexually explicit or threatening language will not be tolerated. All staff should use language appropriate for school situations as indicated by school codes of conduct;
3. Harassing, insulting or attacking others personally is unacceptable;
4. Staff must respect all copyright issues regarding software, information, and attributions of authorship. The intellectual property of another individual or organization cannot be used without their permission. The law prohibits duplicating software for profit, making multiple copies for use by different users within an organization, and giving an unauthorized copy to another individual;
5. Computers, network and Internet shall only be used for legal activities. Illegal activities include tampering with computer hardware or software, unauthorized entry into computers, or knowledgeable vandalism or destruction of computer files whether they belong to ANW, individuals, or an organization. Such activity is considered a crime under state and federal law;
6. Avoid the known or inadvertent spread of computer viruses by following ANW virus protection procedures. "Computer viruses" are programs that have been developed as pranks and can destroy valuable programs and data. Deliberate attempts to degrade or disrupt system performance of ANW computers or network or any other computer system or network on the Internet by spreading computer viruses is considered criminal activity under state and federal law;
7. Scan any computer disks with virus detection software before installation and execution;
8. Prevent the introduction of viruses, attempts to breach system security, or other malicious tampering with any of ANW electronic systems;
9. Report any viruses, tampering, or other system breaches to the system administrator immediately;
10. Each staff member is fully responsible for the use of his/her account. Violations of this policy that can be traced to an individual account will be treated as the sole responsibility of the owner of that account. Staff members should not give their password to anyone other than District administration or the technology coordinator;
11. Do not access pornographic, obscene or sexually explicit web sites; do not download, upload or otherwise distribute any pornographic, obscene or sexually explicit materials; if material is inappropriate for viewing and discussion in a classroom, then it is inappropriate to view it or have it on your computer;
12. Avoid unauthorized commercial use of ANW computers, networks, or Internet;

GD Computer, Network and Internet Acceptable Use Policy

13. Do not waste ANW computer, network and Internet resources;
14. Do not post private information including home address, telephone number, school address or photography of any other person;
15. Do not post chain letters or Email messages;
16. Do not use ANW network system for political lobbying, but may use the system to communicate with elected representative and to express opinions on political issues.
17. A staff member's right to use ANW computers, network and Internet resources ends once the staff member terminates employment or once such privileges are revoked by ANW.

Any suspected violation of this policy will be investigated by ANW administration. Prior to the conclusion of the investigation, the staff member should be informed of the suspected violation and given an opportunity to offer an explanation. Violation of this policy will result in disciplinary action. Disciplinary action will initially be considered at the building level in keeping with existing procedures and practices regarding inappropriate language and behavior. A confirmed violation of this policy may result in (a) suspension of computer, network and Internet use privileges; (b) suspension or termination with ANW; (c) such other discipline as the ANW Board or administration deem appropriate; and (d) in some circumstances, criminal or civil liability for violation of state or federal law. When appropriate, law enforcement agencies shall be notified of violations of this policy.

Each ANW staff member shall be provided with a copy of this policy. By using ANW's Computers, all staff members consent to this Computer, Network and Internet Acceptable Use Policy.

This policy supercedes the Computer Usage and Software Policy dated 01/01/98.

Adopted by the ANW Board of Education on January 22, 2003.

## **INTERNET SAFETY POLICY For ANW Special Education Cooperative #603**

### **Introduction:**

It is the policy of **ANW Special Education Cooperative #603** to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].

### **Definitions:**

Key terms are as defined in the Children's Internet Protection Act.

### **Access to Inappropriate Material:**

To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information.

Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors.

Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.

### **Inappropriate Network Usage:**

To the extent practical, steps shall be taken to promote the safety and security of users of the **ANW Special Education Cooperative #603** online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications.

Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called 'hacking,' and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

### **Supervision and Monitoring:**

It shall be the responsibility of all members of the **ANW Special Education Cooperative #603** staff 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 or otherwise modifying any technology protection measures shall be the responsibility of the Director or designated representatives.

### **Adoption**

The Board of **ANW Special Education Cooperative #603** adopted this Internet Safety Policy at a public meeting, following normal public notice, on **Feb, 10, 2010**.

### **CIPA definitions of terms:**

**TECHNOLOGY PROTECTION MEASURE.** The term “technology protection measure” means a specific technology that blocks or filters Internet access to visual depictions that are:

1. **OBSCENE**, as that term is defined in section 1460 of title 18, United States Code;
2. **CHILD PORNOGRAPHY**, as that term is defined in section 2256 of title 18, United States Code; or
3. Harmful to minors.

**HARMFUL TO MINORS.** The term “harmful to minors” means any picture, image, graphic image file, or other visual depiction that:

1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
2. Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
3. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

**SEXUAL ACT; SEXUAL CONTACT.** The terms “sexual act” and “sexual contact” have the meanings given such terms in section 2246 of title 18, United States Code.