

## ACCEPTABLE USE POLICY FOR STAFF

**Guidelines for Acceptable Use of Technology (AUP):** Employees of the Doniphan West School District USD #111 are provided access to networked computers, software, and peripherals. The use of computers is for the performance of school-related or job-related duties only. Acceptance of the guidelines is indicated by signing below. Employee's, must indicate acceptance of these guidelines as a condition to being granted access to computers and the network.

**Purpose:** This document is an application for the use of technology media resources, information networks, and Internet resources in the Doniphan West School District USD #111. It establishes policy and provides information about acceptable use while using school resources and is therefore called an Acceptable Use Policy (AUP).

Users must sign this AUP prior to being provided access to technology resources. A copy will be kept at the Doniphan West Schools' District Office.

### Terms and Conditions for the use of school and district technology media resources, information networks and the Internet.

Please read the following carefully before signing this document. The signature at the end of this document is legally binding and indicates the party who signed has read the terms and conditions carefully and understands the significance.

District staff members will access technology resources, information networks and the Internet and with this comes responsibility. This document explains responsibilities and the possible consequences of any action in violation of the rules established in this AUP.

Technology resources and information networks may provide access, unauthorized or inadvertent access to sensitive, confidential or restricted files. Anyone accessing or copying such information is in violation of this AUP. Staff members may face disciplinary action. Staff members may have their access terminated. Files on the network or residing on any technology media are subject to control and inspection by administration without user consent.

### **Terms and Conditions**

- 1. Acceptable Use :** The use of any district-owned equipment must be in support of education and research. Use of other organization's network or technology resources must comply with the rules appropriate for that network. Transmission or reception of any materials in violation of any U.S. or state regulation is prohibited. This includes but is not limited to the following: copyrighted material, threatening or obscene material, viruses or unsolicited files, or material protected by trade secret. Use for product advertisement or political lobbying is also prohibited.

2. **Privileges** : All technology resources purchased by USD #111 remain the property of the district. All technology loaned to staff are subject to be returned upon administration request or at the end of district employment. The use of technology resources, information networks, and the Internet is a privilege, not a right and inappropriate use will result in a cancellation of those privileges.
  
3. **Etiquette on the Network** : Users are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to the following:
  - a) **Be polite.** Do not be abusive in messages to others. Respect opinions and beliefs. The Internet is a global community representing many races, religions, and social structures.
  - b) **User Appropriate language.** Do not respond to or engage in personal verbal attacks. Do not swear, use vulgarities, or any other inappropriate language. Avoid using slang and all caps as it is often misunderstood or may be offensive to others. Correct English is the international language of the Internet.
  - c) User may not use a district computer, network or electronic storage device to store, send, or receive, messages or materials which are pornographic or inappropriate
  - d) **Do not reveal** personal (home) addresses or phone numbers as well as those of others, unless on a secure site (<https://>) However, use caution any time personal information is requested on a website in order to avoid possible identity theft.
  - e) **Falsify** his/her identity over the network, share network and computer passwords.
  - f) Use or **transmit** any material in violation of federal, state, or local law. This includes, but is not limited to, copyrighted materials, threatening or obscene materials, or material protected by trade regulations.
  - g) Place **unlawful information**, programs, or other data which is considered unlawful on any computer or network system/storage device.
  - h) Change, manipulate, or move secure information or data on any district computer(s) or network system.
  - i) District technology may not be used for personal profit, commercial purposes, or political purposes.
  - j) Use or abuse a district computer, network, or electronic storage device in a way that would cause:
    - a. physical damage to hardware or software,
    - b. partial or complete erasure of programs or data,
    - c. malfunction or loss of use of equipment, computer, or network services.
  - k) Users may not download and/or install any software, instant messengers, peer-to-peer software, shareware, freeware; or subscribe to free site that may be considered suspicious and untrusting, etc. without the permission of the system administrator, superintendent, or building principal.

- l) Staff are prohibited to hook any computer, notebook, or storage device to the network without proper permission and consideration by the system administrator. The purpose is to ensure network access control and to provide a stable network infrastructure.
  - m) Any person responsible for damage to any part of the district's computer system shall be required to reimburse the district for the reasonable cost of repair or replacement which is the result in whole or in part of the willful destruction of property.
  - n) **E-mail is not guaranteed to be private.** People who operate the system do have access to all mail unless it is encrypted first. Messages relating to, or in support of illegal activities may be reported to authorities.
  - o) **Do not use the network in such a way** that would disrupt the use of the network by others or violate the Privacy Act, a federal law. Do not attempt to access files or use applications that are outside the scope of learning objectives. This includes, but is not limited to, school administrative information, student or teacher records and the network operating system. All communications and files accessible via the network should be assumed to be private.
- 4. Security :** Security on any technology system is a high priority, especially when the system involves many users. Users must notify a system administrator or the principal if they feel they have identified a security problem on the school network(s) or the Internet. Do not demonstrate the problem to other users. Do not use another individual's account. Attempts to login to the school network(s) or the Internet as a system administrator, whether on or off district property, may result in cancellation of use privileges and disciplinary action. Any user identified as a security risk or having a history of problems with technology or network systems may be denied access to school technology resources.
- 5. Vandalism :** Vandalism will result in cancellation of privileges. Vandalism is defined as any malicious attempt to harm or destroy data or equipment belonging to the USD #111 Doniphan West School District, or another user, the Internet, or any of the organizations or other networks that are connected to the Internet backbone. This includes, but is not limited to, the uploading or creation of computer viruses. Users are not allowed to use or install software unless specifically approved by administration. Users are not allowed to subscribe to non-educational lists unless specifically approved by administration. Users are not allowed to engage in non-educational, on-line activities that will monopolize connections or the network.

**Federal Law :** This policy has been created to comply with CIPA (Children's Internet Protection Act), which was signed into law on December 21, 2000. An Internet filter/monitor will be in place on all student/staff computers in the district. While a filter limits inappropriate Internet use, it does not replace the importance of Internet safety education. USD #111 Doniphan West School District will offer opportunities to all students, staff, and possibly parents to

educate them about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response. As partners, we can begin the important task of introducing the Internet to your child in a structured way.

Listed below are a few sites for parents to learn more about the Internet and how to guide your child if you are interested.

<http://www.common sense media.org/>  
<http://www.getnetwise.org/>  
<http://www.safekids.com/>  
<http://www.netsmartz.org/>  
<http://www.ed.gov/pubs/parents/internet/>

The U.S. Government, as well as the state government, has developed criminal statutes to promote responsible use of information services across networks. The consequences are severe for “hackers,” whether malicious or not. Title 18, United States Code, Section 1343 (covering wire fraud) and Section 1030 (covering computer-related fraud) carry stiff penalties. Penalties range from 1 to 30 years in prison and \$250,000 to \$1,000,000 in fines. The U.S. Government has also created a “cyberspace” task force to investigate possible violations of U.S. Code and gather evidence. The use of computer networks leaves an “electronic trail.”

6. **Warranties :** USD #111 Doniphan West School District makes no warranties of any kind, whether expressed or implied, for the technology resources and network services it provides. The district or its employees will not be responsible for any damages suffered. This includes loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by negligence or user errors or omissions. Use of any information obtained via technology resources is at the user’s own risk. The district specifically denies any responsibility for the accuracy or quality of information obtained through its information resources.
7. **Negligence :** If technology resources are damaged, lost or stolen, it is the ultimate responsibility of the employee to pay for the damage or to replace the item(s).
8. **Exception of Terms and Conditions :** All terms and conditions as stated in this document are applicable to the USD #111 Doniphan West School District. They shall be governed and interpreted in accordance with the laws of the state of Kansas and the United States of America.
9. **No Right to Privacy :** All forms of electronic communications will be monitored by the district to ensure that systems are being used only for authorized purposes. Illegal activities will be reported to the appropriate authorities. Students and employees of the district shall have no expectation of privacy for information that is generated, placed in memory, or stored on a

district computer or storage device. Students and employees waive any right to privacy in communications, and consent to the access and disclosure of email messages by authorized employees.

**10. Confidential Student or Employee Information:** Employees shall secure files containing confidential student or confidential employee information. The method for securing files shall be determined by the district system administrator in consultation with the superintendent, or the superintendent's designee.

**11. Passwords/Coding/Encryption/Security:** Employees shall not share user passwords to each other to help gain access to the network resources. All district personnel should exercise "due diligence" regarding password security.

I, the undersigned, understand and will abide by the above Terms and Conditions for the use of USD #111 Doniphan West School District technology resources, networks and the Internet. I further understand that any violation of the policies above is unethical and may also constitute a criminal offense. Should I commit any violation, my access privileges may be revoked and/or appropriate disciplinary as well as legal action taken.

**I understand and will comply with the conditions listed above.**

\_\_\_\_\_  
Employee Signature

\_\_\_\_\_  
Date