WINFIELD UNIFIED SCHOOL DISTRICT 465
1407 WHEAT ROAD
WINFIELD, KS 67156

Acceptable Use and Internet Safety Policy

Acceptable Use Policy (AUP) of Computers, Networks, Internet, Electronic Mail, and Other Online Services

The district will provide administrators, teachers, and other employees' access to computers, networks, Internet, e-mail, and employee data systems through the district's internal and external accounts. The use of computers, networks, the Internet, e-mail, and other on-line services shall be consistent with the educational objectives of the district.

Administrative Implemental Procedures:

1. Services. The school district encourages employees to use computers, networks, Internet, e-mail, and other online services and apply these tools in appropriate ways to the performance of tasks associated with their positions and assignments.

2. Appropriate Use. Employees shall communicate with electronic tools in a professional manner consistent with state laws and district policies governing the behavior of school employees and with federal laws governing copyright. E-mail and other electronic tools shall not be improperly utilized to disclose confidential information about district employees or to disclose information from student education records in violation of the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g, as amended, and its interpretive regulations, 34 C.F.R. § 99.1, *et seq*. This shall not apply to the student information system program or other district administrative software that is to be used by authorized employees in a manner that complies with FERPA and its interpretive regulations.

3. Public Communication. Communication over networks should not be considered to be private. The district network administrator(s) from time to time may review directories or messages to ascertain compliance with network guidelines for acceptable use. The network administrator(s) may delete files that exceed manageable storage level or are deemed inappropriate.

4. Student Access. Regardless of any measures implemented by the District as may be required by the Children's Internet Protection Act, teachers, administrators, and others who make decisions regarding student access to the Internet shall be diligent in monitoring and supervising student computer use. To the extent possible, students' use of the Internet shall be structured in ways that point students to those resources that have been evaluated prior to use. Students shall not be allowed to utilize electronic communications unless a signed consent is on file. A family's right to decide whether or not to sign the Student Access Contract for their student shall be supported and respected. Permission is not transferable from one student to another and may not be shared.

5. Violations. Employees who violate this policy will be subject to appropriate disciplinary action, up to and including termination.

6. Inappropriate Use. The following uses of school-provided access to computers, networks, Internet, e-mail, and other online services are not permitted on the part of district employees:
    a. Accessing, uploading, downloading, or distributing pornographic, obscene, or sexually explicit material;
    b. Transmitting obscene, abusive, sexually explicit, or threatening language;
    c. Violating any local, state, or federal statute;

d. Accessing another employee's materials, information, or files without permission from the employee or the appropriate network administrator or principal;
e. Violating copyright or otherwise using the intellectual property of another individual or organization without permission;
f. Using others' passwords and allowing students to use staff members' passwords;
g. Vandalizing (any unauthorized access and/or malicious attempt to damage computer hardware/software or networks or destroying the data of another user) including creating, uploading, or intentionally introducing viruses;
h. Intentionally wasting limited resources;
i. Using the network for commercial purposes;
j. Harassing, insulting, or attacking others;
k. Using e-mail lists from the district's Internet site, network, or servers to create mailing lists for non-school purposes;
l. Gaining unauthorized access to resources or entities;
m. Invading the privacy of individuals;
n. Improperly altering the setup of computers (e.g., desktops, icons, wallpapers, screensavers, or installed software) as determined by the network administrator;
o. Failing to follow district policies while using computers or failing to follow any other policies or guidelines established by district administration or the user's supervisor and failure to follow instructions of supervisors; and
p. Seeking to gain or gaining unauthorized access to information resources or other computing devices.

7. Security. Users are responsible for maintaining a safe, secure environment:
   a. Users will keep passwords secure; and
   b. Users will change passwords when directed by the network administrator.

8. Security Risk. Any user identified as a security risk or having a history of problems with other computer systems may be denied access.

9. Copyright law shall be followed.

10. Disclaimer. The district makes no warranties of any kind, whether express or implied, for the access it is providing, nor will it be responsible for any damages suffered. This includes loss of data resulting from delays, nondeliveries, misdeliveries, or service interruptions caused by its own negligence or user errors or omissions. Use of any information obtained via the Internet is at the user's risk. The district denies any responsibility for the accuracy or quality of information obtained through its system. The district is not liable for any commercial transactions conducted through its system.

11. Statements of Personal Belief. Any statement of personal belief found on computers, networks, the Internet, e-mail, other on-line services, or any other telecommunication system shall be implicitly understood to be representative of the author's individual point of view, and not that of USD 465, its administrators, teachers, staff, or the participating school. No representations to the contrary shall be published without written approval from the designated district-level administrator(s). Principals, district-level administrators, or their designees may review all content in any Internet or on-line accounts paid for, in whole or in part, by the district or any school, without notice of any kind.

12. Employee Access Contract & Annual Review: School and district office administrators will review acceptable use policies annually with staff.

Internet Safety Policy

Introduction

It is the policy of USD 465 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 for adults 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 USD 465 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.

Education, Supervision and Monitoring

It shall be the responsibility of all members of the USD 465 staff to educate, supervise and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Information Technology Department or designated representatives.

The Information Technology Department or designated representatives will provide age appropriate training for students who use the USD 465 Internet facilities. The training provided will be designed to promote the USD 465 commitment to:

a. The standards and acceptable use of Internet services as set forth in the USD 465 Acceptable Use and

Internet Safety Policy;

b. Student safety with regard to:

i. safety on the Internet;
ii. appropriate behavior while on online, on social networking Web sites, and
in chat rooms; and
iii. cyberbullying awareness and response.

c. Compliance with the E-rate requirements of the Children's Internet Protection Act ("CIPA").

Following receipt of this training, the student will acknowledge that he/she received the training, understood it, and will follow the provisions of the District's acceptable use policies.

Adoption

This Internet Safety Policy was adopted by the Board of USD 465 at a public meeting, following normal public notice, on 6-11-2012.

_____

*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.

WINFIELD UNIFIED SCHOOL DISTRICT 465
1407 WHEAT ROAD
WINFIELD, KS 67156

Please sign the following Acceptable Use and Internet Safety Policy form and turn it in to the appropriate designated supervisor and keep the guidelines for your reference.

Acceptable Use and Internet Safety Policy Form

As a user of the Winfield School District equipment, I hereby agree to comply with the above stated rules. I understand my rights and the guidelines for use on the equipment and that I will be held liable for any violations. I accept and understand the Acceptable Use and Internet Safety Policy Form.

I have read and agree to the user terms described in this agreement.

Name _____ (Please Print)

Signature _____

School Name _____

Date _____