

USD #218 Employee Technology Use Handbook

New technology is always on the horizon. An attempt to identify all technologies and list possible misuses of them is impossible. Therefore, throughout this technology handbook, the term “technology” will be used to reference all existing and new devices or systems that are now used or that will be invented in the future. Such technologies now include computers, handheld devices, cell phones, iPods, and digital cameras. What is to come is unknown. The policies and procedures in this handbook all apply to any form of technology whether it is specifically mentioned or not.

Employees shall have no expectation of privacy when using district e-mail or other official communication systems. E-mail messages shall be used to conduct approved and official district business. All employees must use appropriate language in all messages. Employees are expected to conduct themselves in a professional manner and to use the system according to these guidelines or other guidelines published by the administration.

Any e-mail or computer application or information in district computers or computer systems is subject to monitoring by the administration. The district retains the right to duplicate any information in the system or on any hard drive. Employees who violate district computer policies are subject to disciplinary action.

Computers are provided for faculty to use to complete work-related duties. Therefore, personal computers should not be brought to school. Cell phones and other technologies should be used only in emergencies and should never interfere with the learning environment.

Children’s Internet Protection Act– The district shall implement the Children’s Internet Protection Act (CIPA). The superintendent shall develop a plan to implement the Children’s Internet Protection Act. This plan shall be on file with the board clerk and in each school office with Internet access, and copies shall be available. The superintendent shall ensure compliance with CIPA by completing Federal communication Commission forms as required.

DISCIPLINARY ACTION RELATED TO MISUSE OF TECHNOLOGY

Employee failure to abide by the Acceptable Use Policy may result in disciplinary action following disciplinary procedures established in the district with the following qualifications:

1. Employee misuse of the system is defined in the Acceptable Use Policy. The definitions therein are not exclusive. If an employee is clever enough to invent a new way of misusing technology, and it is reasonable that the employee would know what he/she is doing is improper, the employee may nonetheless be disciplined.
2. Employee use of the district's technology is a privilege granted to employees by the district, not a legal right. Since it is a privilege, the district may restrict any employee's use of technology or the net system if the employee abuses that privilege.

Disciplinary Action

Consequences for the violation of the Acceptable Use Policy will be determined by the employee's supervisor and the superintendent, and may include, but are not limited to, a verbal warning, loss of technology privileges, or termination of employment.

TECHNOLOGY USE

Use of District and Personal Technology

- **Use of District Technology/Privacy Rights:**

Computer systems are for educational and professional use by district employees only. All information created by staff and students shall be considered district property and shall be subject to unannounced monitoring by district administrators. The district retains the right to discipline any student, up to and including expulsion, and any employee, up to and including termination, for violations of this policy.

Copyright:

Software acquired by staff using either district or personal funds, and installed on district technology, must comply with copyright laws. Proof of purchase (copy or original) must be available upon request.

Installation:

No software, including freeware or shareware, may be installed on any district computer until cleared by the network administrator. The network administrator will verify the compatibility of the software with existing software and hardware, and prescribe installation and de-installation procedures. Employees shall not install software on district computers or computer systems.

Hardware:

Employees shall not install unapproved hardware on district computers or make changes to software settings that support district hardware.

- **Use of Personal Technology**

Computers are provided for employees to use to complete work-related duties. Therefore, personal computers should not be brought to school. Cell phones and other technologies should be used only in emergencies and should never interfere with the learning environment.

TECHNOLOGY USE

Technology Materials

Audits:

The network administrator may conduct periodic audits of software installed on district equipment to verify legitimate use.

Privacy Rights:

Employees and/or students shall have no expectation of privacy when using district e-mail or other official communication systems. Any e-mail or computer application or information in district computers or computer systems is subject to monitoring by the administration.

Ownership of Employee/Student-Produced Computer Materials:

Computer materials or devices created as part of any assigned district responsibility or classroom activity undertaken on school time shall be the property of the board.

“NETIQUETTE” ON THE INTERNET

All users of the USD #218 technology and networks are expected to abide by the generally accepted rules of network etiquette (netiquette). Informal rules of behavior have evolved for the use of and communication on the Internet and other on-line services. These rules of behavior include, but are not limited to, the following:

1. Be polite. Do not write or send abusive messages to others.
2. Use appropriate language. Do not swear, use vulgarity, or any inappropriate language.
3. Do not reveal your personal address or phone numbers or those of others.
4. Note that electronic mail (e-mail) is not guaranteed to be private. People who operate the system do have access to mail. Messages relating to or in support of illegal activities may be reported to the authorities.
5. All communications and information accessible via the network should be assumed to be private property which is subject to copyright laws.
6. Do not place unlawful information on any network system.
7. Keep paragraphs and messages short and to the point. Focus on one subject per message.
8. Do not use the network in such a way that would disrupt the use of the network by other users (i.e., downloading very large files during prime time, sending mass e-mail messages).
9. Adult patrons, visitors, or other guests allowed network access are serving as ambassadors and representatives of the district. Conduct and message content on the network should positively reflect on the district's reputation.

POLICY FOR ACCEPTABLE USE OF TECHNOLOGY AND NETWORKS

The following policy for acceptable use of technology and networks (including e-mail, all software, video and digital equipment, and the Internet) shall apply to all district administrators, faculty, staff, and students.

1. The user shall not erase, change, rename, or make unusable anyone's computer files, programs, or disks (except for authorized staff members).
2. The user shall not let other persons use his/her name, logon, password, or files for any reason (except for authorized staff members).
3. The user shall not use or try to discover another's password or in any way access another person's e-mail or other files (except for authorized staff members).
4. The user shall not change any file that does not belong to the user.
5. The user shall not falsify his identity to others.
6. The user shall not use district school technology or networks for any non-instructional or non-administrative purpose (i.e., games or activities for personal use).
7. The user shall not use technology for unlawful purposes, such as illegal copying or installation of software.
8. The user shall not copy, change, or transfer any software or documentation provided by district schools, teachers, or other students without permission.
9. The user shall not write, produce, generate, copy, propagate, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any computer's memory, file system, or software. Such software is often called a bug, virus, Trojan Horse, or similar name.
10. The user shall not deliberately use technology to annoy or harass others with language, images, innuendoes, or threats. The user shall not deliberately access, send or create any obscene or objectionable information, language, or images.
11. The user shall not intentionally damage the technology, the network system, damage information belonging to others, misuse system resources, or allow others to misuse system software.
12. The user shall not tamper with computers, networks, printers, or other associated equipment, except as directed by the teacher.
13. The user shall not circumvent security measures on school or remote computers or networks.
14. The user desiring to take home technology equipment (hardware or software) must first have an Acceptable Use agreement on file and signed agreeing to the terms. Any take-home technology shall be used in the same manner as if it were at school. Technology equipment will only be checked out at the end of the school day and must be returned before school begins the next morning.
15. All information on any school or district network is considered property of USD #218 unless specified by law, students and staff shall have no expectation of privacy for any information created, stored, or used on any district computer system.
16. The user shall not use the technology or network in ways that violate federal, state, or local statutes.
17. While resources should be consulted for various assignments, words or ideas cannot be copied directly and they should be properly cited, with credit given to the original authors. Images taken from another source must also be cited properly. (Plagiarism)

KANSAS COMPUTER CRIME LAW

K.S.A. 21-3755. COMPUTER CRIME; CRIMINAL COMPUTER ACCESS.

(a) As used in this section, the following words and phrases shall have the meaning respectively ascribed thereto:

(1) **“Access”** means to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or computer network.

(2) **“Computer”** means an electronic device which performs work using programmed instruction and which has one or more of the capabilities of storage, logic, arithmetic, or communication and includes all input, output, processing, storage, software, or communication facilities which are connected or related to such a device in a system or network.

(3) **“Computer Network”** means the interconnection of communication lines, including microwave or other means of electronic communication, with a computer through remote terminals, or a complex consisting of two or more interconnected computers.

(4) **“Computer Program”** means a series of instructions or statements in a form acceptable to a computer which permits the functioning of a computer system in a manner designed to provide appropriate products from such computer systems.

(5) **“Computer Software”** means computer programs, procedures, and associated documentation concerned with the operation of a computer system.

(6) **“Computer System”** means a set of related computer equipment or devices and computer software which may be connected or unconnected.

(7) **“Financial Instrument”** means any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card, debit card, or marketable security.

(8) **“Property”** includes, but is not limited to, financial instruments, information, electronically produced or stored data, supporting documentation, and computer software in either machine or human readable form.

(9) **“Services”** includes, but is not limited to, computer time, data processing and storage functions and other uses of a computer, computer system, or computer network to perform useful work.

(10) **“Supporting Documentation”** includes, but is not limited to, all documentation used in the construction, classification, implementation, use or modification of computer software, computer programs, or data.

COMPUTER CRIME IS:

(1) Intentionally, and without authorization, gaining or attempting to gain access to and damaging, modifying, altering, destroying, copying, disclosing or taking possession of a computer, computer system, computer network, or any other property.

(2) Using a computer, computer system, computer network or any other property, for the use of devising or executing a scheme or artifice with the intent to defraud or for the purpose of obtaining money, property, services, or any other thing of value by means of false or fraudulent pretense or representation;

OR

21-3755 (Con't.)

(3) Intentionally exceeding the limits of authorization and damaging, modifying, altering, destroying, copying, disclosing, or taking possession of a computer, computer system, computer network, or any other property.

(c)(1) Computer crime which causes a loss of the value of less than \$500 is a ***class A nonperson misdemeanor***.

(2) Computer crime which causes a loss of the value of at least \$500, but less than \$25,000, is a ***severity level 9, nonperson felony***.

(3) Computer crime which causes a loss of the value of \$25,000 or more is a ***severity level 7, nonperson felony***.

(d) In any prosecution from computer crime, it is a defense that the property or services were appropriated openly and avowedly under a claim of title mead in good faith.

(e) Criminal computer access is intentionally, fraudulently, and without authorization, gaining or attempting to gain access to any computer, computer system, computer network, or to any computer software, program, documentation, data or property contained in a computer, computer system, or computer network. Criminal computer access is a ***class A nonperson misdemeanor***.

(f) This section shall be part of, and supplemental to, the Kansas criminal code.

History: L. 1985, ch. 108, s 1; L. 1992, ch. 298, s 51; L. 1993, ch. 291, s 93; L. 1994, ch. 291, s 34; July 1.

ACCEPTABLE USE OF TECHNOLOGY AND NETWORKS

EMPLOYEE'S AGREEMENT

In order to make sure that all members of the district community understand and agree to these rules of conduct, the district asks that you as an employee sign the following:

Acceptable Use of Technology

I agree not to hold USD #218 Public Schools, or any of its employees, or any of the institutions or networks providing access to networks, responsible for the performance of the system or the content or costs of any material accessed through it.

As a district employee, I have read the terms and conditions for Elkhart Schools' technology use and Internet access. I understand that this free access is designed for educational purposes. However, I also recognize that it is impossible to restrict access to all controversial materials, and I will not hold Elkhart Schools responsible for materials acquired or sent via the network.

I agree to abide by the Acceptable Use of Technology policies.

District Technology Checkout

I sign this form as a condition of checking out technology to take home as needed for academic and professional use. I assume responsibility for any damage to and responsibility for, the repair and/or replacement of the technology while it is in my custody. I assume responsibility for any unauthorized use of the technology while it is in my custody and will supervise its use to see that the technology is used only for academic and/or professional purposes. I will assume responsibility to pay for any damage, repair, and/or replacement for any damage done to district hardware which may result from my use of the technology. I will assume responsibility to pay for any damage, repair, and/or replacement for any damage done to district software which may result from a virus introduced as a result of my use of the technology. I will not add, remove, or copy any programs, software, or information in a manner which may violate copyright laws. I have reviewed the Kansas law included in the acceptable use policy.

I agree to abide by the District Technology Checkout policy

Release of Material on the Internet

I hereby give my consent to, and authorize publication on the district computer system of any work product made by me or publication of any school photograph in which I may appear. I realize any person or persons may view the web site on which my work product or image may appear. By signing this form, I agree to release and forever discharge Elkhart school, its agents, servants and employees, members of the USD #218 School Board and its members, from any and all claims, demands, losses, damages, costs, expenses, and attorney's fees growing out of, caused by, or arising in any manner out of the posting, publication, or use of my work product or image on the district's computer system.

I agree to allow the publication of my work and/or image on the district computer system.

I do NOT agree to allow the publication of my image on the district computer system.

Employee's Signature: _____ Date: _____

This form will be retained on file by authorized faculty designee for duration of applicable computer/network/Internet use.