

## **TECHNOLOGY USAGE** ***(Acceptable Use Policy)***

For the purposes of this regulation and related policy and forms, the following terms are defined:

*User* -- any person who is permitted by the district to utilize any portion of the district's technology resources, including but not limited to students, employees, School Board members and agents of the school district.

*User Identification (ID)* -- any identifier which would allow a user access to the district's technology resources, or to any program, including but not limited to e-mail and Internet access.

*Password* -- a unique word, phrase or combination of alphabetic, numeric and non-alphanumeric characters used to authenticate a user ID as belonging to a user.

### **Student Users**

No student will be given access to the district's technology resources until the district receives a *User Agreement* signed by the student and the student's parent(s), guardian(s), or person(s) standing in the place of a parent. Students who are 18 or who are otherwise able to enter into an enforceable contract may sign the *User Agreement* without additional signatures. Students who do not have a *User Agreement* on file with the district may be granted permission to use district technology by the superintendent or designee in unusual situations.

### **Employee Users**

No employee will be given access to the district's technology resources before the district has a signed *User Agreement* on file.

Authorized employees may use the district's technology resources for reasonable, incidental personal purposes as long as the use does not violate any provision of district policy, regulation or procedure, hinder the use of the district's technology for the benefit of its students or waste district resources. Any use which jeopardizes the safety, security or usefulness of the district's technology is considered unreasonable. Any use which interferes with the effective and professional performance of the employee's job is considered unreasonable.

All employees must model the behavior expected of students, exhibit the same judgment as expected of students and serve as role models for students. Because computers are shared resources, it is not appropriate for an employee to access, view, display, store, print or disseminate information via district resources, including e-mail or Internet access, which students or other users could not access, view, display, store, print or disseminate, unless authorized by the district.

FILE: EHB-R  
Critical

Student teachers, interns, volunteers, substitutes, etc., are considered as employees for the purposes of network access.

### **Board Member Users**

Members of the School Board may be granted user privileges, including an electronic mail address, upon completion of a *User Agreement*. Board members will set an example of responsible use and will abide by district policies, regulations and procedures. Board members will comply with the Missouri Sunshine Law.

### **External Users**

Consultants, counsel, independent contractors, and other persons having professional business with this school district may also be granted user privileges at the discretion of the superintendent or designee, subject to completion of a *User Agreement* and for the sole, limited purpose of conducting business with the school. External users must abide by all laws, district policies, regulations and procedures.

### **Privacy**

A user does not have a legal expectation of privacy in the user's electronic communications or other activities involving the district's technology resources.

All district technology resources are considered school property. The district may maintain or improve technology resources at any time. The district may remove, change or exchange hardware or other technology between buildings, classrooms, employees, students or any other user at any time, without prior notice. Authorized district personnel may load or delete new programs or information, install new equipment, upgrade any system or enter any system to correct problems at any time.

The district may examine all information stored on district technology resources at any time. The district may monitor employee and student technology usage. Electronic communications, all data stored on the district's technology resources, and downloaded material, including files deleted from a user's account, may be intercepted, accessed or searched by district administrators or designees at any time.

### **Violations of Technology Usage Policies and Procedures**

Use of the district's technology resources is a privilege, not a right. A user's privileges may be suspended pending an investigation concerning use of the district's technology resources. Any

violation of district policy, regulations or procedures regarding technology usage may result in temporary, long-term or permanent suspension of user privileges.

The administration may use disciplinary measures to enforce district policy, regulations and procedures. Students may be suspended or expelled for violating the district's policies, regulations and procedures. Employees may be disciplined or terminated for violating the district's policies, regulations and procedures. Any attempted violation of district policy, regulations or procedures, regardless of the success or failure of the attempt, may result in the same discipline or suspension of privileges as that of an actual violation.

### ***Sanctions***

1. Violations may result in a loss of access.
2. Additional disciplinary action may be determined at the building level in line with existing practice regarding inappropriate language or behavior.
3. When applicable, law enforcement agencies may be involved.

### **Content Filtering and Monitoring**

The district will monitor the on-line activities of minors and operate a technology protection measure ("filtering/blocking device") on all computers with Internet access, as required by law. The filtering/blocking device will attempt to protect against access to visual depictions that are obscene, harmful to minors and child pornography, as required by law. Evasion or disabling, or attempting to evade or disable, a filtering/blocking device installed by the district is prohibited.

The superintendent or designee, or the district's technology administrator may disable the district's filtering/blocking device to enable an adult user access for bona fide research or other lawful purposes. In making decisions to disable the district's filtering/blocking device, the administrator shall consider whether the use will serve a legitimate educational purpose or otherwise benefit the district.

### **General Rules and Responsibilities**

The following rules and responsibilities will be followed by all users of the district technology resources:

- a. Applying for a user ID under false pretenses is prohibited.
- b. Using another person's user ID and/or password is prohibited.

FILE: EHB-R  
Critical

- c. Sharing one's user ID and/or password with any other person is prohibited.
- d. A user will be responsible for actions taken by any person using the ID or password assigned to the user.
- e. Deletion, examination, copying or modification of files and/or data belonging to other users without their prior consent is prohibited.
- f. Mass consumption of technology resources that inhibits use by others is prohibited.
- g. Noneducational Internet usage is prohibited except for reasonable, incidental personal purposes.
- h. Use of district technology for soliciting, advertising, fund-raising, commercial purposes or for financial gain is prohibited, unless authorized by the district.
- i. Accessing fee services without permission from an administrator is prohibited. A user who accesses such services without permission is solely responsible for all charges incurred.
- j. Users are required to obey all laws, including criminal, copyright, privacy, defamation and obscenity laws. The school district will render all reasonable assistance to local, state or federal officials for the investigation and prosecution of persons using district technology in violation of any law.
- k. Accessing, viewing or disseminating information using district resources, including e-mail or Internet access, that is pornographic, obscene, child pornography, harmful to minors, obscene to minors, libelous, pervasively indecent or vulgar, or advertising any product or service not permitted to minors is prohibited.
- l. Accessing, viewing or disseminating information on any product or service not permitted to minors is prohibited unless under the direction and supervision of district staff for curriculum-related purposes.
- m. Accessing, viewing or disseminating information using district resources, including e-mail or Internet access, that constitutes insulting or fighting words, the very expression of which injures or harasses other people (e.g. threats of violence, defamation of character or of a person's race, religion or ethnic origin); presents a clear and present likelihood that, because of their content or their manner of distribution, will cause a material and substantial disruption of the proper and orderly operation and discipline of the school or school activities; or will cause the commission of unlawful acts or the violation of lawful school regulations is prohibited.

- n. Any use which has the purpose or effect of discriminating or harassing any person or persons on the basis of race, color, religion, sex, national origin, ancestry, disability, age, pregnancy, or use of leave protected by the Family and Medical Leave Act or the violation of any person's rights under applicable laws is prohibited. *See policy AC and regulation AC-R.*
- o. Any unauthorized, deliberate, or negligent action which damages or disrupts technology, alters its normal performance, or causes it to malfunction is prohibited, regardless of the location or the duration of the disruption.
- p. Users may only install and use properly licensed software, audio or video media approved for use by the district. All users will adhere to the limitations of the district's technology licenses. Copying for home use is prohibited unless permitted by the district's license, and approved by the district.
- q. At no time will district technology or software be removed from the district premises, unless authorized by the district.
- r. All users will use the district's property as it was intended. Technology or technology hardware will not be lifted, moved or relocated without permission from an administrator. All users will be held accountable for any damage they cause to district technology resources.
- s. All damages incurred due to the misuse of the district's technology will be charged to the user. The district will hold all users accountable for the damage incurred and will seek both criminal and civil remedies, as necessary.
- t. Electronic resources provided for home access are for the exclusive use of CPS students, staff and Board of Education members.
- u. Web pages by teachers shall be hosted on servers maintained by the district or on an approved site. All district web pages including teacher web pages shall be approved for compliance with the Americans with Disabilities Act (ADA). Content of web pages hosted on school web sites needs to be education/focused.

### **Technology Security and Unauthorized Access**

All users shall immediately report any security problems or misuse of the district's technology resources to a teacher or administrator.

FILE: EHB-R  
Critical

No person will be given access to district technology if he/she is considered a security risk by the superintendent or designee.

- a. Use of district technology resources in attempting to gain or gaining unauthorized access to any technology system or the files of another is prohibited.
- b. Use of district technology to connect to other systems, in evasion of the physical limitations of the remote system, is prohibited.
- c. The unauthorized copying of system files is prohibited.
- d. Intentional or negligent attempts, whether successful or unsuccessful, to interfere with the ability of others to utilize any district technology are prohibited.
- e. Any attempts to secure a higher level of privilege on the technology resources without authorization are prohibited.
- f. The introduction of computer “viruses,” “hacking” tools, or other disruptive/destructive programs into a school computer, the school network, or any external networks is prohibited.

**On-Line Safety - Disclosure, Use, and Dissemination of Personal Information**

- a. All students will be instructed on the dangers of sharing personal information about themselves or others over the Internet.
- b. Student users are prohibited from sharing personal information about themselves or others over the Internet, unless authorized by the district.
- c. Student users shall not agree to meet with someone they have met on-line without parental approval.
- d. A student user shall promptly disclose to his/her teacher or another school employee any message the user receives that is inappropriate or makes the user feel uncomfortable.
- e. Users shall receive or transmit communications using only district-approved and district-managed communication systems. For example, users may not use messaging, videoconferencing or chat services, except in special cases where arrangements have been made in advance and approved by the district.

- f. All district employees will abide by state and federal law and Board policies and district rules, including but not limited to, policy JO and regulation JO-R, when communicating information about personally identifiable students.
- g. Employees shall not transmit confidential student information using district technology, unless designated for that use. Employees will take precautions to prevent negligent disclosure of student information or student records.
- h. No curricular or non-curricular publication distributed using district technology will include the address, phone number or e-mail address of any student without permission.

### **Electronic Mail**

A user is responsible for all electronic mail (“e-mail”) originating from the user’s ID or password.

- a. Forgery or attempted forgery of e-mail messages is illegal and prohibited.
- b. Unauthorized attempts to read, delete, copy or modify e-mail of other users are prohibited.
- c. Users are prohibited from sending unreasonable amounts of unsolicited electronic mail unless the communication is a necessary, employment-related function, or an authorized publication.
- d. All users must adhere to the same standards for communicating on-line that are expected in the classroom, and consistent with district policies, regulations and procedures.

### **Exceptions**

Exceptions to district rules will be made for district employees or agents conducting an investigation of a use which potentially violates the law, district policy, regulations or procedures. Exceptions will also be made for technology administrators who need access to district technology resources to maintain the district’s resources or examine and delete data stored on district computers as allowed by the district’s retention policy.

### **Waiver**

Any user who believes he/she has a legitimate reason for using the district’s technology in a manner which may violate any of the district’s adopted policies, regulations and procedures may request a waiver from the building principal, superintendent or their designees. In making the decision to grant a waiver to a student, the administrator shall consider the purpose, age, maturity, and level of supervision involved.

FILE: EHB-R  
Critical

### **No Warranty/No Endorsement**

The district makes no warranties of any kind, whether expressed or implied, for the services, products or access it provides. The district's technology resources are available on an "as is, as available" basis.

The district is not responsible for loss of data, delays, non-deliveries, mis-deliveries or service interruptions. The district does not guarantee the accuracy or quality of information obtained from the Internet, or use of its technology resources. Access does not include endorsement of content or the accuracy of the information obtained.

\* \* \* \* \*

**Note: The reader is encouraged to review administrative procedures and/or forms for related information in support of this policy area.**

Approved: 03/11/2002

Legal Refs: §§ 170.051, 171.011, 177.011, .031, 431.055, .056, 537.525, 542.402, 569.093 - .099, 570.223, 610.010 - .028, RSMo.  
Chapter 573, Revised Statutes of Missouri (*passim*)  
P. L. 106-554, Children's Internet Protection Act  
P. L. 99-508, 1000 Stat. 1848, Electronic Communications Privacy Act  
Family Educational Rights and Privacy Act, 20 U.S.C. § 1232(g)  
Federal Wiretap Act, 18 U.S.C. § 2511 *et.seq.*  
Stored Communications Act, 18 U.S.C. § 2701 *et.seq.*  
*Reno v. ACLU*, 117 S.Ct. 2329 (1997)  
*Ginsberg v. New York*, 390 U.S. 629 (1968)  
*FCC v. Pacifica Foundation*, 438 U.S. 726 (1978)  
*Hazelwood v. Kuhlmeier*, 484 U.S. 260 (1988)  
*Bethel Sch. District No. 403 v. Fraser*, 478 U.S. 675 (1986)  
*Sony Corporation of America v. Universal City Studios, Inc.*, 464 U.S. 417 (1984)  
*Henerey by Henerey v. City of St. Charles School District*, 200 F.3d. 1128 (8<sup>th</sup> Cir. 1999)  
*Bystrom v. Fridley High Sch.*, 822 F.2d 747 (8<sup>th</sup> Cir. 1987)  
*Urofsky v. Gilmore*, \_\_ F.3d \_\_ (4<sup>th</sup> Cir. 2000)  
*J.S. v. Bethlehem Area Sch. Dist.*, \_\_ A.2d \_\_ (Pa. Comw. 2000)  
*Beidler v. North Thurston Sch. Dist.*, No. 99-2-00236-6 (Wash. Super. Ct. July 18, 2000)

Columbia School District No. 93 , Columbia, Missouri