TECHNOLOGY USAGE

The Golden City R-III School District's technology exists for the purpose of enhancing the educational opportunities and achievement of district students. Research shows that students who have access to technology improve achievement. In addition, technology assists with the professional enrichment of the staff and increases engagement of students' families and other patrons of the district, all of which positively impact student achievement. The district will periodically conduct a technology census to ensure that instructional resources and equipment that support and extend the curriculum are readily available to teachers and students.

The purpose of this policy is to facilitate access to district technology and to create a safe environment in which to use that technology. Because technology changes rapidly and employees and students need immediate guidance, the superintendent or designee is directed to create procedures to implement this policy and to regularly review those procedures to ensure they are current.

Definitions

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

Technology Resources B Technologies, devices and services used to access, process, store or communicate information. This definition includes, but is not limited to: computers; modems; printers; scanners; fax machines and transmissions; telephonic equipment; mobile phones; audio-visual equipment; Internet; electronic mail (e-mail); electronic communications devices and services, including wireless access; multi-media resources; hardware; and software. Technology resources may include technologies, devices and services provided to the district by a third party.

User B 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) B Any identifier that 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 B A unique word, phrase or combination of alphabetic, numeric and non-alphanumeric characters used to authenticate a user ID as belonging to a user.

Authorized Users

The district's technology resources may be used by authorized students, employees, School Board members and other persons approved by the superintendent or designee, such as consultants, legal counsel and independent contractors. All users must agree to follow the district=s policies and procedures and sign or electronically consent to the district's User Agreement prior to accessing or using district technology resources, unless excused by the superintendent or designee.

Use of the district=s technology resources is a privilege, not a right. No potential user will be given an ID, password or other access to district technology if he or she is considered a security risk by the superintendent or designee.

User 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 including, but not limited to, voice mail, telecommunications, e-mail and access to the Internet or network drives. By using the district's network and technology resources, all users are consenting to having their electronic communications and all other use monitored by the district. A user ID with e-mail access will only be provided to authorized users on condition that the user consents to interception of or access to all communications accessed, sent, received or stored using district technology.

Electronic communications, downloaded material and all data stored on the district=s technology resources, including files deleted from a user=s account, may be intercepted, accessed, monitored or searched by district administrators or their designees at any time in the regular course of business. Such access may include, but is not limited to, verifying that users are complying with district policies and rules and investigating potential misconduct. Any such search, access or interception shall comply with all applicable laws. Users are required to return district technology resources to the district upon demand including, but not limited to, mobile phones, laptops and tablets.

Technology Administration

The Board directs the superintendent or designee to assign trained personnel to maintain the district=s technology in a manner that will protect the district from liability and will protect confidential student and employee information retained on or accessible through district technology resources.

Administrators of district technology resources may suspend access to and/or availability of the district=s technology resources to diagnose and investigate network problems or potential violations of the law or district policies and procedures. All district technology resources are considered district property. The district may remove, change or exchange hardware or other technology

between buildings, classrooms or users at any time without prior notice. Authorized district personnel may install or remove programs or information, install equipment, upgrade any system or enter any system at any time.

Content Filtering and Monitoring

The district will monitor the online activities of minors and operate a technology protection measure (Acontent filter@) on the network and all district technology with Internet access, as required by law. In accordance with law, the content filter will be used to protect against access to visual depictions that are obscene or harmful to minors or are child pornography. Content filters are not foolproof, and the district cannot guarantee that users will never be able to access offensive materials using district equipment. Evading or disabling, or attempting to evade or disable, a content filter installed by the district is prohibited.

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

Online Safety, Security and Confidentiality

In addition to the use of a content filter, the district will take measures to prevent minors from using district technology to access inappropriate matter or materials harmful to minors on the Internet. Such measures shall include, but are not limited to, supervising and monitoring student technology use, careful planning when using technology in the curriculum, and instruction on appropriate materials. The superintendent, designee and/or the district's technology administrator will develop procedures to provide users guidance on which materials and uses are inappropriate, including network etiquette guidelines.

All minor students will be instructed on safety and security issues, including instruction on the dangers of sharing personal information about themselves or others when using e-mail, social media, chat rooms or other forms of direct electronic communication. Instruction will also address cyberbullying awareness and response and appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms.

This instruction will occur in the district's computer courses, courses in which students are introduced to the computer and the Internet, or courses that use the Internet in instruction. Students are required to follow all district rules when using district technology resources and are prohibited from sharing personal information online unless authorized by the district.

All district employees must abide by state and federal law and Board policies and procedures when using district technology resources to communicate information about personally identifiable students to prevent unlawful disclosure of student information or records.

All users are prohibited from using district technology to gain unauthorized access to a technology system or information; connect to other systems in evasion of the physical limitations of the remote system; copy district files without authorization; interfere with the ability of others to utilize technology; secure a higher level of privilege without authorization; introduce computer viruses, hacking tools, or other disruptive/destructive programs onto district technology; or evade or disable a content filter.

Closed Forum

The district=s technology resources are not a public forum for expression of any kind and are to be considered a closed forum to the extent allowed by law. The district=s webpage will provide information about the school district, but will not be used as an open forum.

All expressive activities involving district technology resources that students, parents/guardians and members of the public might reasonably perceive to bear the imprimatur of the district and that are designed to impart particular knowledge or skills to student participants and audiences are considered curricular publications. All curricular publications are subject to reasonable prior restraint, editing and deletion on behalf of the school district for legitimate pedagogical reasons. All other expressive activities involving the district=s technology are subject to reasonable prior restraint and subject matter restrictions as allowed by law and Board policies.

Records Retention

Trained personnel shall establish a retention schedule for the regular archiving or deletion of data stored on district technology resources. The retention schedule must comply with the *Public School District Records Retention Manual* as well as the *General Records Retention Manual* published by the Missouri Secretary of State.

In the case of pending or threatened litigation, the district's attorney will issue a litigation hold directive to the superintendent or designee. The litigation hold directive will override any records retention schedule that may have otherwise called for the transfer, disposal or destruction of relevant documents until the hold has been lifted by the district's attorney. E-mail and other technology accounts of separated employees that have been placed on a litigation hold will be maintained by the district's information technology department until the hold is released. No employee who has been so notified of a litigation hold may alter or delete any electronic record that falls within the scope of the hold. Violation of the hold may subject the individual to disciplinary actions, up to and including

termination of employment, as well as personal liability for civil and/or criminal sanctions by the courts or law enforcement agencies.

Violations of Technology Usage Policies and Procedures

Use of technology resources in a disruptive, inappropriate or illegal manner impairs the district=s mission, squanders resources and shall not be tolerated. Therefore, a consistently high level of personal responsibility is expected of all users granted access to the district=s technology resources. Any violation of district policies or procedures regarding technology usage may result in temporary, long-term or permanent suspension of user privileges. User privileges may be suspended pending investigation into the use of the district=s technology resources.

Employees may be disciplined or terminated, and students suspended or expelled, for violating the district=s technology policies and procedures. Any attempted violation of the district's technology policies 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. The district will cooperate with law enforcement in investigating any unlawful use of the district's technology resources.

Damages

All damages incurred by the district due to a user's intentional or negligent misuse of the district's technology resources, including loss of property and staff time, will be charged to the user. District administrators have the authority to sign any criminal complaint regarding damage to district technology.

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, nondeliveries, misdeliveries or service interruptions. The district does not endorse the content nor guarantee the accuracy or quality of information obtained using the district's technology resources.

* * * * * * *

Note: ***The reader is encouraged to check the index located at the beginning of this section for other pertinent policies and to review administrative procedures and/or forms for related information.***

FILE: EHB
Critical

Adopted: June 21, 2016

Revised:

Cross Refs: AC, Prohibition against Discrimination, Harassment and Retaliation
GBCC, Staff Use of Communication Devices
GBH, Staff/Student Relations
IGAEB, Teaching about Human Sexuality
IGDB, Student Publications
IGDBA, Distribution of Noncurricular Student Publications
JFCF, Hazing and Bullying
JG-R1, Student Discipline
JO, Student Records
KB, Public Information Program

MSIP Refs: 6.4, 6.8

Legal Refs: ' ' 170.051, 182.827, 431.055, 537.525, 542.402, 569.095 - .099, 610.010 - .028, RSMo.
Chapter 109, RSMo.
Chapter 573, RSMo.
Electronic Communications Privacy Act, 18 U.S.C. ' ' 2510 - 2520
Stored Communications Act, 18 U.S.C. ' ' 2701 - 2711
Family Educational Rights and Privacy Act, 20 U.S.C. ' 1232g
No Child Left Behind Act of 2001, 20 U.S.C. ' ' 6301 - 7941
Children=s Internet Protection Act, 47 U.S.C. ' 254(h)
47 C.F.R. ' 54.520
Federal Rule of Civil Procedure 34
City of Ontario v. Quon, 130 S. Ct. 2619 (2010)
Reno v. ACLU, 521 U.S. 844 (1997)
Hazelwood Sch. Dist. v. Kuhlmeier, 484 U.S. 260 (1988)
Bethel Sch. Dist. No. 403 v. Fraser, 478 U.S. 675 (1986)
Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417 (1984)
FCC v. Pacifica Foundation, 438 U.S. 726 (1978)
Ginsberg v. New York, 390 U.S. 629 (1968)
Biby v. Bd. of Regents of the Univ. of Nebraska, 419 F.3d 845 (8th Cir. 2005)
Henerey v. City of St. Charles Sch. Dist., 200 F.3d 1128 (8th Cir. 1999)
Bystrom v. Fridley High Sch. Ind. Sch. Dist., 822 F.2d 747 (8th Cir. 1987)
Beussink v. Woodland R-IV Sch. Dist., 30 F. Supp. 2d 1175 (E.D. Mo 1998)

Golden City R-III School District, Golden City, Missouri