TECHNOLOGY USAGE

The Smithville R-II School District's technology exists for the purpose of maximizing 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 Board 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.

Definitions

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

Technology Resources – Technologies, devices and resources 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, audio-visual equipment, Internet, electronic mail, electronic communications devices and services, multi-media resources, hardware and software.

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 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 - 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 such as consultants, legal counsel and independent contractors. All users must agree to follow the district's policies and procedures. Unless authorized by the superintendent or designee, all users must have a signed *User Agreement* on file with the district before they are allowed access to district technology resources.

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/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 technology resources, including 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 or searched by district administrators or designees at any time in the regular course of business to protect users and district equipment. Any such

search, access or interception will be reasonable in inception and scope and shall comply with all applicable laws.

Technology Administration

The Board directs the superintendent or designee to create procedures governing technology usage and 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 computer 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 maintain or improve technology resources at any time. The district may remove, change or exchange hardware or other technology between buildings, classrooms or users at anytime without prior notice. Authorized district personnel may install or remove new programs or information, install new equipment, upgrade any system or enter any system to correct problems at any time.

Content Filtering and Monitoring

The district will monitor the on-line activities of minors and operate a technology protection measure ("filtering/blocking device") on the network and/or all computers with Internet access, as required by law. The filtering/blocking device will be used to protect against access to visual depictions that are obscene or harmful to minors or are child pornography, as required by law. Filtering/Blocking devices are not foolproof, and the district cannot guarantee that users will never be able to access offensive materials using district equipment. Evasion or disabling, or attempting to evade or disable, a filtering/blocking device installed by the district is prohibited.

The superintendent, designee or the district's technology administrator may disable the district's filtering/blocking device to enable non-student user access for bona fide research or for 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.

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 web-page will provide information about the school district, but will not be used as an open forum.

All expressive activities involving district's 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 that complies 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 schedules 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 computer 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, manifestly 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.

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.

Student Users

No student will be given access to the district's technology resources until the district receives *User Agreements* signed by the student and the student's parent/guardian. Students who do not have a *User Agreement* on file with the district may be granted permission to use the district's technology resources by the superintendent or designee.

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 user does not violate any provision of district policies or procedures, hinder the use of the district's technology resources for benefit of its students or waste district resources. Any use that jeopardizes the safety, security or usefulness of the district's technology resources or

interferes with the effective and professional performance of the employee's job is considered unreasonable. Unless authorized by the district, employees may not access, view, display, store, print or disseminate information using district technology resources that students or other users could not access, view, display, store, print or disseminate.

External Users

Consultants, legal counsel, independent contractors and other persons having professional business with the district may 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 and procedures.

General Rules and Responsibilities

The following rules and responsibilities will apply to all users of the district's technology resources:

1. Applying for a user ID under false pretenses or using another person's ID or password is prohibited.

2. Sharing user IDs or passwords with others is prohibited and users will be responsible for using the ID or password. A user will not be responsible for theft of passwords and IDs, but may be responsible if the theft was the result of user negligence.

3. Deleting, examining, copying or modifying files or data belonging to other users without their prior consent is prohibited.

4. Mass consumption of technology resources that inhibits use by others is prohibited.

5. Use of district technology for soliciting, advertising, fundraising, commercial purposes or financial gain is prohibited, unless authorized by the district.

6. 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.

7. 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.

8. The district prohibits the use of district technology resources to access, view or disseminate information 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.

9. 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.

10. The district prohibits the use of district technology resources to access, view or disseminate information that constitutes insulting or fighting words, the very expression of which injures or harasses other people (e.g., threat 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, they 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 district policies and procedures.

11. The district prohibits any use that violates any person's rights under applicable laws, and specifically prohibits any use that has the purpose or effect of discriminating or harassing any person 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.

12. The district prohibits any unauthorized intentional or negligent action that damages or disrupts technology, alters its normal performance or causes it to malfunction. The district will hold users responsible for such damage and will seek both criminal and civil remedies, as necessary.

13. Users may only install and use properly licensed software, audio or video media purchased by the district or 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.

14. At no time will district technology or software be removed from the district premises, unless authorized by the district.

15. All users will use the district's property as it was intended. Technology resources will not be moved or relocated without permission from an administrator. All users will be held accountable for any damage they cause to district technology resources.

16. File-sharing programs and peer to peer software will not be tolerated. The use of "file-sharing programs" is prohibited regardless of their use or intent.

17. Downloading or streaming any type of music/video related files for personal use is prohibited.

Technology Security and Unauthorized Access

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

2. Use of district technology resources in attempting to gain or gaining unauthorized access to any technology system or the files of another is prohibited.

3. Use of district technology to connect to other systems, in evasion of the physical limitations of the remote system, is prohibited.

4. The unauthorized copying of system files is prohibited.

5. Intentional or negligent attempts, whether successful or unsuccessful, to interfere with the ability of others to utilize any district technology are prohibited.

6. Any attempts to secure a higher level of privilege on the technology resources without authorization are prohibited.

7. The introduction of computer viruses, hacking tools or other disruptive or destructive programs into a district computer, network or any external networks is prohibited.

8. Any attempt to circumvent content filtering by utilizing proxies is prohibited.

Online Safety and Confidentiality

Curricular or noncurricular publications distributed using district technology will comply with the law and Board policies on confidentiality.

All district employees will abide by state and federal law, Board policies and district rules when using district technology resources to communicate information about personally identifiable students. Employees will take precautions to prevent negligent disclosure of student information or student records.

All students will be instructed on the dangers of sharing personal information about themselves or others over the Internet and are prohibited from sharing such information unless authorized by the district. Student users shall not agree to meet with someone they have met online without parental approval and must promptly disclose to a teacher or another district employee any message the user receives that is inappropriate or makes the user feel uncomfortable.

Electronic Mail

A user is responsible for all e-mail originating from the user's e-mail account.

1. Forgery or attempted forgery of e-mail messages is illegal and is prohibited.

2. Unauthorized attempts to read, delete, copy or modify e-mail of other users are prohibited.

3. Users are prohibited from sending unsolicited mass e-mail.

4. All users must adhere to the same standards for communicating electronically that are expected in the classroom and that are consistent with district policies and procedures.

5. Students must obtain permission from the superintendent or designee before sending any districtwide e-mail messages.

Exceptions

Exceptions to district rules will be made for district employees or agents conducting an investigation of a use that potentially violates the law, district policies 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 or she has a legitimate educational purpose for using the district's technology in a manner that may violate any of the district's policies or 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.

Adopted: May 17, 2000
Revised: January 15, 2003
Revised May 29, 2014
MSIP Refs: 6.4, 6.8
Smithville R-II School District, Smithville, Missouri