Policy EHB: TECHNOLOGY USAGE

Wright City R-II

Original Adopted Date: 08/08/2002 | **Last Revised Date:** 01/23/2018

Status: ADOPTED

The Wright City R-II 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 – Technologies, devices and services used to access, process, store or communicate information. This definition includes, but is not limited to: tablets, iPods/iPads, eReaders, 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 – 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, community 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 string of characters that a user must enter to gain access to a resource.

Authorized Users

The district's technology resources may be used by authorized students, employees, School Board members, community 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. Authorized district personnel 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 ("content 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, as required by law. 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.

The superintendent or designee will create a procedure that allows students, employees or other users to request that the district review or adjust the content filter to allow access to a website or specific content.

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 web page 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.

Inventory and Disposal

The district will inventory all district technology equipment in accordance with the district's policies on inventory management. Technology resources that are no longer needed will be disposed of in accordance with law and district policies and procedures related to disposal of surplus property.

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.

For Office Use Only: [EHB-C.WRT]

Student Users

All student users and their parents/guardians must sign or electronically consent to the district's User Agreement prior to accessing or using district technology resources, unless otherwise excused by this policy or the superintendent or designee. Students who are 18 or who are otherwise able to enter into an enforceable contract may sign or consent to 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 the district's technology resources by the superintendent or designee.

Employee Users

All employees must sign or electronically consent to the district's User Agreement prior to accessing or using district's technology resources. 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 or procedure, hinder the use of the district's technology resources for the 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 employee's supervisor in advance, 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 business with the district may be granted user privileges at the discretion of the superintendent or designee after consenting to the district's User Agreement and for the sole, limited purpose of conducting business with the school. Members of the community will be allowed access to the district's computers during "community usage" hours. The user must sign or electronically consent to the district's User Agreement before using the equipment and a staff member must be present at all times. 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. User identifications and passwords are the property of the Wright City School District and should never be shared. A user may only use his or her own user identification or password and should never provide his or her user identification or password to any user other than the technology department staff.

2. Sharing user IDs or passwords with others is prohibited except when shared with the district's technology department for the purpose of support. Individuals who share IDs or passwords may be disciplined and will be held responsible for any actions taken by those 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. Users must adhere to district policies procedures and other district guidelines. All users shall immediately report any security problems or misuse of the district's technology resources to an administrator or teacher.

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

5. Deleting, examining, copying or modify district files or data without authorization is prohibited.

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

7. Unauthorized mass consumption of technology resources, including mass electronic mailings is prohibited.

8. Use of district technology for soliciting, advertising, fundraising, commercial purposes or financial gain is prohibited, unless authorized by the district or in accordance with policy KI. Use of district technology resources to advocate, support or oppose any ballot measure or candidate for public office is prohibited.

9. 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.

10. Users are required to obey all laws, including criminal, copyright, privacy, defamation and obscenity laws. The 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.

11. 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, or pervasively indecent or vulgar.

12. 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.

13. 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., 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, 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.

14. 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 against or harassing any person on the basis of race, color, religion, sex, national origin, ancestry, disability, age, genetic information, pregnancy or use of leave protected by the Family and Medical Leave Act (FMLA).

15. 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.

16. Users may install and use only properly licensed software and 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.

17. Installation of personal hardware is prohibited unless authorized by the district.

18. Software installed on district equipment must be approved prior to installation by the technology department.

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

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

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 or any personally-owned device in an attempt to hack into or gain unauthorized access to any technology resources or to connet to other systems either inside or outside of the district is prohibited.

3. The unauthorized copying of software, system files or other district-owned resources is prohibited.

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

5. Users will be granted access privileges to district technology resources as determined appropriate by the superintendent or designee. Any attempt to secure a higher level of privilege without authorization is prohibited.

6. The introduction of computer viruses, Malware, hacking tools or other disruptive or destructive programs onto district resources or any external resources is prohibited.

7. Disabling, altering or uninstalling district antivirus software is prohibited unless authorized by the district.

8. Attempting to compromise the district's network security by any means is prohibited.

9. Attempting to bypass the district's content filter 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 about themselves or others over the Internet, 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 and Messaging

1. A user is generally responsible for all e-mail and other electronic messages originating from the user's accounts; however, users will not be held responsible when the messages originating from their accounts are the result of the account being hacked.

2. All electronic accounts and the contents thereof are the property of the Wright City School District.

3. Electronic messages should not be regarded as private, as the district cannot guarantee the confidentiality of e-mail and other electronic messages.

4. The district reserves the right to monitor, inspect, disclose or discontinue electronic messages without consent or notice.

5. Forgery or attempted forgery of electronic messages is illegal and prohibited.

6. Unauthorized attempts to read, delete, copy or modify electronic messages of other users are prohibited.

7. Users are prohibited from sending unsolicited mass e-mail or other electronic messages. The district considers more than five addresses per message, per day a violation, unless the communication is a necessary, employment-related function or an authorized publication. Electronic messages containing religion or other potentially controversial subjects are prohibited unless authorized by administration.

8. Accessing or utilizing personal e-mail accounts (i.e., not district issued) on district resources is prohibited unless authorized by administration.

9. 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.

10. Users must obtain permission from the superintendent or designee before sending any districtwide electronic messages.

Communication Devices

Employees and others to whom the district provides mobile phones or other electronic communication devices must use them professionally and in accordance with district policies, regulations and procedures. These devices shall not be used in a manner that would distract the employee or other user from adequate supervision of students or other job duties.

Personal Electronic Devices

Personally-owned handheld wireless electronic devices including, but not limited to, e-readers, iPods/iPads, tablets and cell phones are permitted for use by staff, students (grades 6-12), guests and other persons approved by the superintendent or designee. Devices with ethernet ports and devices that support USB to ethernet adaptors are prohibited unless approved by the technology department. Examples of prohibited devices include personal laptops and personal chromebooks. Student use of personal electronic devices is subject to individual building guidelines.

Personal handheld electronic devices may only access the Internet through the district's designated guest wireless network and not through personal cellular data plans or other networks available, including other wireless networks and wired networks. Users are prohibited from connecting personal electronic devices to the district's private network.

Technical support will not be provided for personal devices. Users must take full responsibility for setting up and maintaining their personal handheld electronic devices.

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, regulations 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 student's purpose, age, maturity and level of supervision involved.

* * * * * * *

Note: The reader is encouraged to review policies and/or forms for related information in this administrative area.

Administrative Procedure EHB-AP(2): TECHNOLOGY USAGE - (Access to Blocked or Filtered Content)

Wright City R-II

Original Adopted Date: 01/23/2018 **Status:** ADOPTED

This procedure allows students, employees or other users to request that the district review or adjust the content filter to allow access to a website or specific Internet content.

Unblocking Content

District technology users who believe that a website or web content has been inappropriately blocked by the district's content filter must use the following process to request access to the blocked Internet content:

1. Users must submit a request, by e-mail or anonymously in writing, to the superintendent or designee for access. The request should include reasoning in support of the request.

2. Requests will be acted on within ten business days of the superintendent or designee receiving the request. The superintendent or designee may consult the district's attorney prior to making a decision. Unless the request was made anonymously, the user requesting access will be notified of the decision.

3. If access is denied, the user may request to be put on the agenda for the next Board meeting to discuss the issue. The Board has the discretion to grant or deny the agenda request. The requested material will remain blocked until the Board makes a decision, if any.

* * * * * * *

Note: The reader is encouraged to review policies and/or forms for related information in this administrative area.
