TECHNOLOGY USAGE
(Technology Safety)

Definitions

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, authorized contractors, and other authorized agents of the 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.

Closed Forum – a communication device, tool, software, hardware, internet site or account owned and\or operated by a governmental entity that is closed to the public for expressive activities of any kind.

Technology Resources – Technologies, devices, software, 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; telephone equipment; mobile phones; audio-visual equipment; Internet; social media; 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.

Technology Administration

The Board directs the Superintendent or designee to assign trained personnel to maintain the District's technology in a manner that will (a) protect the District from liability, (b) Protect Proprietary software, and (c) protect confidential student and employee information retained or accessible through District technology resources. These trained personnel will

1. 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.
2. establish a retention schedule for the regular archiving or deletion of data stored on District technology resources in accordance with the *Public School District Retention Manual* published by the Missouri Secretary of State.
3. 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, regulations and procedures.
4. install or remove programs or information, install equipment, upgrade any system or enter any system at any time appropriate or necessary.

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. The administrators may also remove, change or exchange hardware or other technology between buildings, classrooms or users at any time without prior notice. When possible, users will be notified of this in advance. However, there may be situations when, at the District may do so without notice.

All District technology resources are considered District property.

Authorized Users

District technology resources may be used by authorized

1. students
2. employees
3. School Board members
4. other persons approved by the Superintendent or designee, such as consultants, legal counsel and independent contractors.

Conditions and Rules of Use

Use of the District's technology resources is a privilege, not a right. Access privileges to technology resources are granted based on the needs of the District. The following rules will be followed by all District technology resource users. If District administrators determine any violation of these conditions or rules may be unlawful, the appropriate law enforcement agency will be contacted. Any possible violation of Board policy will be investigated and may lead to discipline up to and including termination.

1. 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.
2. A user should not have a legal expectation of privacy in any 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.
3. 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 when using District access and/or resources.
4. Users must consent in their *User Agreement* to interception of or access to all communications accessed, sent, received or stored using District technology.
5. The District will only provide a user ID with e-mail access if the user consents to interception of or access to all communications accessed, sent, received or stored using District technology.
6. Passwords for accounts held by Board members will be held by the Superintendent's

Office.

7. No student, employee or other potential user will receive an ID, password or other access to District technology if he or she is considered a security risk by the Superintendent or designee.
8. A user will be responsible for any actions taken by those using the user's ID or password. A user will not be responsible for theft of passwords and IDs unless the theft was the result of user negligence.
9. 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.
10. 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.
11. All users will use the District's property as it was intended.
12. Users are required to return District technology resources to the District upon demand including, but not limited to, mobile phones, laptops, and tablets.
13. Users are responsible for following District asset management and tracking procedures.

Prohibitions

The following are prohibited:

1. Applying for a user ID under false pretenses
2. Using another person's user ID and/or password
3. Sharing user IDs or passwords with others except
   a. when temporary passwords are shared with the District's technology department for the purpose of support.
   b. Teachers may have access to student passwords to ensure that access is appropriate and for instructional purposes.
4. 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.
5. Deleting, examining, copying or modifying District files or data without authorization.
6. Mass consumption of technology resources that inhibits use by others.
7. Use of District technology for soliciting, advertising, fundraising, commercial purposes or financial gain, unless authorized by the District or in accordance with policy KI.
8. Use of District technology resources to advocate, support or oppose any ballot measure or candidate for public office.
9. Accessing fee-based services without permission from an administrator. A user who accesses such services without permission

is solely responsible for all charges incurred.

10. Accessing, viewing or disseminating information using District resources, including e-mail or Internet access that is pornographic, obscene, child pornography, harmful or obscene to minors, libelous, pervasively indecent, vulgar, or otherwise illegal.
11. Accessing, viewing or disseminating information on any product or service not permitted to minors unless under the direction and supervision of District staff for curriculum-related purposes.
12. Accessing, viewing or disseminating information using District Technology resources in a way that constitutes cyber bullying, or insulting or fighting words, by which other people may be harassed or injured or (e.g., threats of violence, defamation of character or of a person's race, religion or ethnic origin)
13. Using District Technology resources to access, view, or disseminate information that may cause a material and substantial disruption of the proper and orderly operation and discipline of the school or school activities, will cause the commission of unlawful acts or the violation of lawful District policies, regulations and procedures.
14. Any use that 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, genetics, 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 (will be addressed as described in policy AC).
15. Any unauthorized, deliberate or negligent action that damages or disrupts technology, alters its normal performance, or causes it to malfunction regardless of the location or the duration of the disruption.
16. Copying software or media in audio or visual format for home or other use unless permitted by the District's license and approved by the District.
17. Removing District technology or software from District premises, unless authorized by the District.
18. Lifting, moving, or relocating Technology hardware without permission from a building administrator. All users will be held accountable and will be charged for any damage they cause to District technology resources. The District will seek both criminal and civil remedies, as necessary.

Student Users

1. All student users under age 18 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.
2. All student users under age 18 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.

3. 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.
4. 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.

Employee Users

1. No employee will be given access to the District's technology resources unless the employee agrees to follow the District's User Agreement prior to accessing or using the District's technology resources.
2. 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, regulations or procedures, hinder the use of the District's technology resources for the benefit of its students or waste District resources.
3. 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.
4. 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.
5. Users will be granted access privileges to District technology resources after approval by their supervisor and by the Technology Services department. The procedure for requesting access is available from the Technology Services department.
6. Any attempts to secure a higher level of privilege than currently approved without authorization is prohibited.

Board Member Users

Upon completing an annual *User Agreement,* Board members may be granted user privileges, including an e-mail address. Board members will set an example of responsible use, will abide by District policies, regulations and procedures, and will comply with the Missouri Sunshine Law.

External Users

The Superintendent or designee has discretion to grant user privileges to consultants, legal counsel, independent contractors and other persons having business with the District, after consenting to the District's User Agreement and for the sole, limited purpose of conducting business with the District. External users must abide by all laws, the District policies, regulations and

procedures.

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. No person will be given access to District technology if he or she is considered a security risk by the Superintendent or designee. The following actions are prohibited:

1. Use of District technology resources to gain or attempt to gain unauthorized access to any technology system or the files of another user;
2. Use of District technology to connect to other systems, in evasion of the physical limitations of the remote system by using a personal wireless account to access sites not allowable if you were using the District's filtered system;
3. The unauthorized copying of system files;
4. Intentional or negligent attempts, whether successful or unsuccessful, to interfere with the ability of others to utilize any District technology;
5. Any attempt to secure a higher level of access privilege than approved by the Superintendent or designees.
6. The introduction of computer viruses, hacking tools or other disruptive or destructive programs into a District computer, network, or any external networks.

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.

Because the District's technology is a shared resource, the content filters will apply to all District computers with Internet access. 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 user 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

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

1. supervising and monitoring student technology use
2. careful planning when using technology in the curriculum
3. instruction on appropriate materials.
4. procedures to provide users guidance on which materials and uses are inappropriate, including network etiquette guidelines.
5. instructing all students on safety and security issues, including (a) appropriate online behavior and (b) 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.
6. instructing all students on cyberbullying awareness and response and appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms.
7. providing instruction 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.
8. instructing and requiring that employees 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

1. gain unauthorized access to a technology system or information
2. connect to other systems in evasion of the physical limitations of the remote system
3. using a personal wireless account to access sites not allowable if you were using the district's filtered system);
4. copy District files without authorization
5. interfere with the ability of others to utilize technology
6. secure a higher level of privilege without authorization
7. introduce computer viruses, hacking tools, or other disruptive/destructive programs onto District technology or internal or external networks.
8. evade or disable a content filter.

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

A. Student Users
   1. All students will be instructed on the dangers of sharing personal information about themselves or others over the Internet.
   2. Student users are prohibited from sharing personal information about themselves or others over the Internet, unless authorized by the District.
   3. Student users shall not agree to meet with someone they have met online without parental approval.

4. A student user shall promptly disclose to his or her teacher or another school employee any message the user receives that is inappropriate or makes the user feel uncomfortable. This would include but not limited to receiving a posting of harmful or cruel text or images which are considered cyber bullying.

B. Employee Users

1. 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.
2. All District employees, including staff assigned to Partner District will abide by state and federal law, Board policies and District rules including, but not limited to, policy JO and regulation in JO-R when communicating information about personally identifiable students.
3. 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.
4. 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.

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 website will provide information about the 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 approval 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 educational 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

A user's privileges may be suspended pending an investigation concerning use of the District's technology resources. Any violation of District policies, regulations or procedures regarding technology usage may result in temporary, long-term or permanent suspension of user privileges.

Employees may be disciplined up to and including termination, and students disciplined or suspended up to expulsion, 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.

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.

Electronic Mail and Messaging

Users must obtain permission from the Superintendent or designee before sending any District wide electronic messages. When communicating electronically, all users must comply with District policies, regulations, and procedures and adhere to the same standards expected in the classroom. 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.

The following actions are prohibited:

1. Forgery or attempted forgery of electronic messages is illegal;
2. Unauthorized attempts to read, delete, copy or modify electronic messages of other users;

3. Sending unsolicited mass e-mail or other electronic messages, unless the communication is a necessary, employment-related function or an authorized publication.

Communication Devices

Employees with mobile phones or other electronic communication devices must use them professionally and in accordance with District Policy GBCC and Regulation GBCC-R. 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.

Damages

All damages incurred by the District due to the misuse of the District's technology resources, including the 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.

Exceptions

An 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, regulations or procedures. An exception 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 they 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.

Date Implemented by the Superintendent: March 13, 2018

Superintendent of Schools