

Technology Usage Policy

Chillicothe R-II School District

The Chillicothe R-II School District recognizes the educational and professional value of electronics-based information technology, both as a means of access to enriching information and as a tool to develop skills that students need.

The district's technology exists for the purpose of maximizing the educational opportunities and achievements of district students. The professional enrichment of the staff and Board, and increased engagement of the students' families and other patrons of the district, are assisted by technology, but are secondary to the ultimate goal of student achievement.

Use of technology resources in a disruptive, noticeably 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. Development of students' personal responsibility is itself an expected benefit of the district's technology program. Any violation of district policy, regulations, or procedures regarding technology usage may result in temporary, long-term or permanent suspension of user privileges. Students may be suspended or expelled. Employees may be disciplined or terminated for violation of district policy, regulation, or procedures regardless of the success or failure of the attempt. This 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 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.

User Agreement

Unless authorized by the superintendent or designee, all users including district employees must have an appropriately signed *User Agreement* on file with the district before they are allowed access to district technology resources. All users must agree to follow the district's policies, regulations, and procedures. The execution of this User Agreement acknowledges the receipt of the District's Technology Usage Policy and the User's agreement to follow and be bound by the same. 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.

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 email or Internet access, which student or other users could not access, view, display, store, print or disseminate, unless authorized by the district.

Board members may be granted user privileges, including an email 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.

Technology Administration

The board directs the superintendent or designee to create rules and procedures governing technology usage in the district to support the district's policy, as needed.

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 or accessible through district technology resources. Trained personnel shall establish a retention schedule for the regular archival 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.

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, regulations and procedures, and to load or delete new programs or information, install new equipment, and upgrade any system by removing, changing, or exchanging hardware between buildings, classrooms, employees, or students at any time.

User Identification and Network Security

The district technology resources may be used by authorized students, employees, School Board members and other persons such as community members, school volunteers, consultants, legal counsel, and independent contractors. Use of the district's technology resources is a privilege, not a right. No student, employee, or other potential user will be given an ID, password, or other access to district technology resources if he/she is considered a security risk by the superintendent or designee. All users shall immediately report any security problems or misuse of the district's technology resources to an administrator or teacher.

Privacy

A user does not have a legal expectation of privacy in the user's electronic mail or other activities involving the district's technology resources. A user ID, if granted, is provided to users of this district's network and technology resources only on condition that the user consents to interception or access to all communications accessed, sent, received, or stored using district technology.

Content Filtering and Monitoring

The district will operate a technology protection measure ("filtering/blocking device") on all computers with Internet access, as required by law. The filtering/blocking device will protect against access to visual depictions that are obscene, harmful to minors and child pornography, as required by law. Because the district's technology is a shared resource, the filtering/blocking device will apply to all computers with Internet access in the district. Evasion or disabling of the filtering/blocking device installed by the district, including attempts to evade or disable, is a serious violation of district policy.

The superintendent or designee 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.

Closed Forum

The district's technology resources, including the district web page, are not a public forum for expression of any kind and are to be considered a closed forum to the extent allowed by law.

Any expressive activity involving district technology resources that students, parents, and members of the public might reasonably perceive to bear the authorization of the school, and which 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.

General Rules and Responsibilities

All users of the district technology resources will follow the following rules and responsibilities:

- a. Applying for a user ID under false pretenses is prohibited.
- b. Using another person's user ID and/or password or any other attempt to gain or gaining unauthorized access to any technology system or files of another is prohibited.
- 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 system files or files and/or data belonging to other users without their prior consent is prohibited.
- f. Any attempt to secure a higher level of privilege on the technology resources

without authorization is prohibited.

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

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

i. Use of district technology for soliciting, advertising, fund-raising, commercial purposes or for financial gain is prohibited, unless authorized by the district.

j. 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.

k. 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.

l. Accessing, viewing, or disseminating information using district resources including email 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.

m. 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.

n. Accessing, viewing or disseminating information using district resources, including email 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 the commission of unlawful acts or the violation of lawful school regulations is prohibited.

o. 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 right under applicable laws is prohibited.

p. Any unauthorized, deliberate, or negligent action, which damages or disrupts technology, alters its normal performance, or causes it to malfunction such as computer "viruses," "hacking" tools, or other disruptive/destructive programs is prohibited, regardless of the location or the duration of the disruption.

q. Users may only install and use properly licenses 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 licenses. Copying for home use is prohibited unless permitted by the district's license, and approved by the district.

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

s. 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.

t. 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.

Online 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 online 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. Employees shall receive or transmit communications using only district-approved and district-managed communication systems for all district-related communication.

f. Students are required to use the district's designated web-based email that is filtered for all school-related projects.

g. Messaging, videoconferencing or chat services, except in special cases where arrangements have been made in advance and approved by the district, are prohibited.

h. All district employees will abide by state and federal law and Board policies and district rules when communicating information about personally identifiable students.

i. 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.

Email

A user is responsible for all electronic mail originating from the user's ID or password.

a. Forgery or attempted forgery of email messages is illegal and prohibited.

b. Unauthorized attempts to read, delete, copy, or modify email of other users are prohibited.

c. Users are prohibited from sending unsolicited mass emails unless the communication is an employment-related function or an authorized publication.

d. All users must adhere to the same standards for communicating online 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.

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.

Your signature(s) on the technology usage contract is (are) legally binding and indicates the party (parties) who signed has (have) read the terms and conditions carefully and understand their significance.