Central R-III School District
Employee Acceptable Use Policy

This acceptable use Policy is a summary of official Board policy 6320 and Regulation 6320. The content and meaning are essentially identical, but all users will be held accountable to all Board policies. The original Board policy and regulation may be found on file in the District administrative office.

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

The district's technology exists for the purpose of maximizing the educational opportunities and achievement of district students. The professional enrichment of the faculty, 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, 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. Development of employees' personal responsibility is itself an expected benefit of the district's technology program.

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

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 which 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's ID as belonging to a user.

Personal Electronic Devices – Include, but are not limited to, electronic communication equipment such as laptops, portable media players, mobile phones, smart phones, tablets, and readers owned by an employee, or student, or a student's parent/guardian.

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 and regulation 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. Technology Administrators 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.

User Identification and Network Security
The district technology resources may be used by authorized students, employees, School Board members, and other persons such as 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 if he/she is considered a security risk by the superintendent or designee.

Users must adhere to district policies, regulations, procedures, and other district rules and guidelines. All users shall immediately report any security problems or misuse of the district's technology resources to an administrator or teacher.

User Agreement
Unless authorized by the superintendent or designee, all users 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.

In addition, all users must recognize that they do not have a legal expectation of privacy in any activities involving the district's technology. In particular, an ID with e-mail access, if granted, is provided to users of the 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. The district reserves the right to search and seize records from all district equipment at any given time.

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.

Content Filtering and Monitoring
The district will monitor the on-line activities of minors and 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 and devices 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.

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. The district website may include the district's address, telephone number, and an e-mail address where members of the public may easily communicate concerns to the administration and the Board.

Any expressive activity involving district technology resources that students, parents, and members of the public might reasonably perceive to bear the imprimatur 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. All other expressive activity involving the district's technology is subject to reasonable prior restraint and subject matter restrictions as allowed by law and Board policies.

Damages

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

No Warranty/Availability/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. Administrators of 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, regulations, and procedures.

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.

General Rules and Responsibilities

The following rules and responsibilities will be followed by all users of the district's technology resources:

1. Applying for a user ID under false pretenses is prohibited.
2. Using another person's user ID and/or password is prohibited unless authorized by the district.
3. Sharing one's user ID and/or password with any other person is prohibited unless authorized by the district.
4. A user will be responsible for actions taken by any person using the ID or password assigned to the user.
5. Deletion, examination, copying, or modification of files and/or data belonging to other users without their prior consent is prohibited.
6. Mass consumption of technology resources that inhibits use by others is prohibited.
7. Unless authorized by the district or building administrator, non-educational internet usage is prohibited.
8. Use of district technology for soliciting, advertising, fundraising, commercial purposes, or for financial gain is prohibited, unless authorized by the district.
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. Accessing, viewing, or disseminating information using district technology resources, including e-mail 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.
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 faculty or staff for curriculum-related purposes.
13. Accessing, viewing, or disseminating information using district technology resources, including e-mail 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 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 school regulations is prohibited.
14. 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 the violation of any person's rights under applicable laws is prohibited.
15. Any unauthorized, deliberate, or negligent action which damages or disrupts technology, alters its normal performance, or causes it to malfunction is prohibited, regardless of the location or the duration of the disruption.
16. Users may only install and use properly licensed software, audio, or video media purchased by the district or approved by the district's Technology Department. 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 technology licenses, and approved by the district. Software not licensed to the district should not be used or installed to any of the district's computers until approved by the Technology Department so that any licensing or compatibility issues have been resolved.
17. At no time will district technology hardware or software be removed from the district's premises, unless authorized by the district.
18. All users will use the district's property as it was intended. Technology hardware will not be moved or relocated without permission from the district's Technology Department. All users will be held accountable for any damage they cause to district technology resources.
19. 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. Any intended damage will be the financial responsibility of the user and accidental damage may be the financial responsibility of the user if good judgment and respect for the equipment was not used.
20. Unauthorized use of any computer/media equipment or accounts is prohibited.
21. Computer/media equipment must not be marked on, colored on, handled roughly, hit, or in any way defaced, altered, or abused.
22. Horseplay of any kind is not allowed around computer/media equipment.
23. Users may not have food or beverages around any computer/media equipment.
24. Users may not move or unplug any computer/media equipment nor adjust computer/media equipment controls without permission from the equipment supervisor and/or district's Technology Department.
25. Employees may only access computer programs that have been assigned by the Technology Department or supervisor. After consulting with the district's Technology Director, exceptions may be approved.

26. Any attempted violation of district policy, regulations, 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.
27. Employees are responsible to delete unwanted files from their network home directories and cloud storage at the end of each school year.
28. District on-line access is provided primarily for educational purposes under the direction of the district's faculty and staff. Non-educational use may be limited at any time by district faculty and staff. Chat lines, Social Networking (or equivalencies), chain letters, chat rooms, or Multiple User Dimensions (MUDs) are prohibited, with the exception of the district's Google Apps for Education. Employees are restricted from "blogging" or utilizing on-line diaries, and are prohibited from viewing or posting to any type of "social networking" sites that are outside the scope of the district's Google Apps for Education.
29. Employees may not set up or use any type of e-mailing accounts or applications not approved by the district.
30. Employees are responsible for scanning any and all portable media (i.e. jump drives, etc.) before using on district computers, including Chromebooks.
31. It is the user's responsibility to report any problems with the computer/media equipment immediately.
32. Users are to utilize the computer/media equipment for its intended purpose.
33. Employees should use computer/media equipment for school-related purposes unless given permission by their building administrator to use for personal use (The Technology Department can deny a user's request to utilize equipment for personal use.).
34. Accidentally accessing inappropriate sites needs to be reported immediately.
35. Users should not assign any unauthorized security protection to any files, programs, or computer/media equipment.
36. Use of obscene, abusive, or otherwise objectionable language, sound, or images in either public or private files or messages is prohibited.
37. Users are solely responsible for the use of their assigned accounts and passwords.
38. Abusive, physical handling of any computer/media equipment by any user is prohibited.
39. Users are not to have installed or use any type of instant messaging services or any other type of e-mail service not directly set up or approved by the Technology Department.

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/she is considered a security risk by the superintendent or designee.

1. Use of district technology resources in attempting to gain or gaining unauthorized access to any technology system or the files of another is prohibited.
2. Use of district technology to connect to other systems, in evasion of the physical limitations of the remote system, is prohibited.
3. The unauthorized copying of system files 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.
5. Any attempts to secure a higher level of privilege on the district's technology resources without authorization are prohibited.
6. The introduction of computer "viruses," "hacking" tools, or other disruptive/destructive programs into a district computer, the district's network, or any external networks is prohibited.

7. Users are not to add, remove, or alter passwords, security measures, configuration settings, or monitoring devices without authorization.

On-Line Safety - Disclosure, Use, and Dissemination of Personal Information, Etiquette, Services, and Privacy

1. Users will be instructed on the dangers of sharing personal information about themselves or others over the internet.
2. Users are prohibited from sharing personal information about themselves or others over the internet, unless authorized by the district. Establishing and viewing of any personal profile sites is strictly prohibited on district computers.
3. An employee shall promptly disclose to an administrator any message the employee receives that is inappropriate or makes the employee feel uncomfortable.
4. Users shall receive or transmit communications using only district-approved and district-managed communication systems. For example, users may not use web-based e-mail, messaging, videoconferencing or chat services, except in special cases where arrangements have been made in advance and approved by the district or building administrator.
5. All district employees will abide by state and federal law, Board policies, and district rules when communicating information about personally identifiable students.
6. 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.
7. 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.
8. Users are expected to be polite. They may not send abusive, insulting, harassing, or threatening messages to others.
9. Users are expected to use appropriate language; language that uses vulgarities or obscenities, libels others, or uses other inappropriate references is prohibited.
10. Users may not reveal their personal addresses, telephone numbers, or the addresses or telephone numbers of students, employees, or other individuals during e-mail transmissions.
11. Users may not use the district's network in such a manner that would damage, disrupt, or prohibit the use of the network by other users.
12. Users should assume that all communications and information is public when transmitted via the network and may be viewed by other users. The Technology Department may access and read e-mail on a random basis.
13. Use of the district's network for unlawful purposes will not be tolerated and is prohibited.
14. The use of an account by someone other than the registered holder will be grounds for loss of access privileges.
15. Students and parents are warned that users may, either intentionally or unintentionally, access textual, graphic, and/or auditory information, which is pornographic, sexually explicit, illegal, defamatory, and otherwise offensive to the user or others. Access to the material is strictly prohibited by this agreement.
16. Violation of any district rules, regulations, or guidelines will result in the loss of the user's privileges to utilize the computer/media equipment (See the Employee User Agreement Violation section.).

On-Line Resources and Services

Access to any on-line information resources and services, MOREnet resources and services, the internet, etc. is an unparalleled opportunity to interact with the world at large. This opportunity brings with it a number of responsibilities. In order to have this privilege, users must follow the stated and expressed guidelines.

1. All rules, regulations, and guidelines for computer/media equipment and all school facilities regulations apply.
2. The opportunity to access on-line information is a privilege, which may be revoked by the Technology Department at any time for abusive, unauthorized, or inappropriate conduct. Such conduct would include, but is not limited to:

    a. The placing or retrieval of any unlawful information on a computer.
    b. Accessing/using another person's account, password, or files.
    c. Using any defamatory, inaccurate, abusive, obscene, profane, sexually orientated, threatening, racially offensive, or illegal materials in either public of private files or messages.
    d. Using an account or computer/media equipment to obtain, view, download, or otherwise gain access to potentially objectionable material, which includes text materials, video images, or sound files that may be considered objectionable.
    e. Using an account or computer/media equipment for commercial or personal financial gain.
    f. Permitting the use of your assigned account and/or password by another user.
3. Because of the potentially large number of individuals who need to use the computer/media equipment for on-line access, student access may be limited.
4. The district reserves the right to inspect any materials stored in files which users have access and will edit or remove any material which administrators believe may be objectionable.
5. The district's on-line access is provided primarily for educational purposes. Non-educational use may be limited.
6. Information services and features provided through the on-line access are intended for the private use of its patrons. Any commercial or other unauthorized use of those materials, in any form, is expressly forbidden.
7. The district does not warrant that the functions of the district's technology will meet any specific requirements users may have, or that it will be error-free or uninterrupted; nor shall it be liable for any direct, or indirect, incidental, or consequential damages (including lost data information, damage to jump drives, etc.) sustained or incurred in connection with the use, operation, or inability to use the district's technology.
8. Rules and regulations of usage are subject to change. All users are subject to these rules and regulations.

E-mail Use

Employees should only use district-provided electronic mail.

Employee user responsibilities include:

1. Protecting your e-mail account and password. You are responsible for the appropriate use of the account.
2. Not interfering with the network traffic by sending broadcasts to lists or individuals.
3. E-mail accounts are to be used only by the registered user.
4. A user is responsible for all electronic mail originating from the user's ID.

5. Forgery or attempted forgery of e-mail messages is illegal and prohibited.
6. Unauthorized attempts to read, delete, copy, or modify e-mail of other users are prohibited.
7. Users are prohibited from sending unsolicited electronic mail to more than 10 addresses per message, per day, unless the communication is a necessary, employment-related function, or an authorized publication.
8. Faculty and staff may not send group building or district-wide e-mails. Requests for group mailing should be sent to the building administrator for approval and will be forwarded at their discretion.
9. Users should refrain from forwarding mailings that do not directly tie to an employment related function and contain music or video clips.
10. 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.
11. Users may only use the district's established format and centralr3.org e-mail address.
12. Users are not to have installed or use any type of instant messaging services or any other type of e-mail service not directly installed or approved by the Technology Department.

Employee Personal Use and Employee Use of Personal Electronic Devices

District computers, network, and internet services are provided for purposes related to district programs and operations, and performance of employees' job responsibilities. Incidental personal use of district computers is permitted as long as such use: 1) does not interfere with the employee's job responsibilities and performance; 2) does not interfere with technology operations or other users; and 3) does not violate this policy and the accompanying rules and guidelines, or any other Board policy, procedure, or district rules. "Incidental personal use" is defined as use by an individual employee for occasional personal communications.

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 e-mail or internet access, which students or other users could not access, view, display, store, print or disseminate, unless authorized by the district.

Employees are not to use computers for personal reasons during supervision or instructional time with students.

Utilization of personal electronic devices is a privilege, not a right, and may be forfeited by failing to abide by the same user responsibilities, rules, and regulations as outlined for district owned devices. Users understand that any violation of these provisions may result in disciplinary action taken against them as described in the Employee User Agreement Violation section.

Further, users understand and agree to the following when using personal electronic devices:

1. The district assumes no liability for lost, stolen, damaged or misplaced devices.

2. The district is not responsible for any loss of information that may arise from the usage of the district's network or any resulting loss, injury, or damages.
3. The district will not be responsible for technological support of the personal electronic devices, and users are required to make sure that devices are free from viruses before bringing them to school.
4. Any problems which arise from the use of a user's account and password are the responsibility of the account holder. Any financial encumbrances of the account are the account holder's sole responsibility. Any misuse of the account will result in suspension of the account privileges.

Employee User Agreement Violation

District-Wide Violation Procedures for Employees*

This procedure accompanies the Employee Acceptable Use Policy and User Agreement. Each employee is responsible for his/her actions and activities involving district computers, networks, and internet services. The Employee Acceptable Use Policy does not attempt to describe every possible prohibited activity by employees. Employees who have questions about whether a particular activity or use is prohibited are encouraged to contact a Building Administrator or the Technology Director.

The following procedures can be implemented when an employee violates the Employee User Agreement.

First Offense: Verbal warning from Building Administrator.

Second Offense: Job Improvement Plan with input, if needed, by the Technology Director.

Third Offense: Continued infractions will result in immediate disciplinary action as determined appropriate by the Building Administrator and Superintendent. Failure to comply with district rules governing computer use may also include suspension and/or termination of employment from the Central R-3 School District. Serious offenses will be treated the same as a third minor offense.

* The district reserves the right to waive any/or all of the above procedures depending on the severity of the infraction. Illegal use of school computers breaking local or federal laws will also result in referral to law enforcement.

Central R-3 School District Technology Usage
Employee User Agreement

I have read the Central R-3 School District Employee Acceptable Use Policy and agree to abide by its provisions. I understand that violations of these provisions may result in disciplinary action taken against me, including but not limited to suspension or revocation of my access to district technology, and termination. I also understand that inappropriate or illegal use of the equipment could result in civil or criminal lawsuits. I also agree not to hold the Central R-3 Schools liable for the gathering of any offensive or undesirable content through the school's electronic media.

I understand that my technology usage is not private and that the school district may monitor my use of district technology, including but not limited to accessing browser logs, e-mail logs, and any other history of use. I consent to district interception of or access to all communications I send, receive, or store using the district's technology resources, pursuant to state and federal law, even if the district's technology resources are accessed remotely.

I understand I am responsible for any unauthorized costs arising from my use of the district's technology resources. I understand that I am responsible for any damages I incur due to my use of the district's technology resources.

_____ _____

Employee Signature Date

_____

Employee Name (Print)