

Central R-III School District

Employee Acceptable Use Policy

This acceptable use Policy is a summary of official Board policies and regulations 6320 and 6321. The content and meaning are essentially identical, but all users will be held accountable to all Board policies. The original Board policies may be found on file in the District administrative office and on the District's Web Page.

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 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 staffs' personal responsibility is itself an expected benefit of the technology department.

Definitions

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

User / Staff / Employee -- 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 districts 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.

Personal Use School unit computers, network and Internet services are provided for purposes related to school programs and operations, and performance of their job responsibilities. Incidental personal use of school 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 system operations or other system users; and 3) does not violate this policy and the accompanying rules, or any other Board policy, procedure or school rules. **"Incidental personal use" is defined as use by an individual employee for occasional personal communications.**

Employee Users

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. ***The District reserves the right to search and seize records and e-mails from all District equipment at any given time.***

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.

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

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.**

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 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 email use activities involving the district's technology. A user ID with e-mail access, 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 in his or her *User Agreement*. ***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 staff 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 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 web page will provide information about the school district, but will not be used as an open forum. The district web page 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 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/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 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.

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.

Rules and Responsibilities

The following rules and responsibilities will be followed by all users of the district 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, fund-raising, 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 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.
11. Accessing, viewing or disseminating information using district 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 staff for curriculum-related purposes.

13. Accessing, viewing or disseminating information using district 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 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. At no time will district technology or software be removed from the district premises, unless authorized by the district.
18. All users will use the district's property as it was intended. Technology or technology hardware will not be moved or relocated without permission from an administrator. All users will be held accountable for any damage they cause to district technology resources.
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.
20. Unauthorized use of any computer/media equipment or accounts is prohibited.
21. Staff should refrain from making Internet purchases that show no direct tie to the staff's job description or educational use.
22. Computers/media equipment must not be marked on, colored on, handled roughly, hit, or in any way defaced, altered or abused. Marks to identify proper wiring connections are permissible.
23. Horseplay of any kind is not allowed around computer/media equipment.
24. Users may not move or unplug any computer/media equipment nor adjust computer equipment controls without permission from the Technology Department.
25. Users may only access computer programs that have been placed on their menus by the system administrator or supervisor. After consulting with the district technology coordinator, exceptions may be approved by a district administrator or the administrator of the building in which the computer is located.
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. Users are responsible to delete unwanted files from their home directories at the end of each school year.
28. Users are restricted from "blogging" or utilizing on line diaries, and are prohibited from viewing or posting to any type of "Social Networking" sites.
29. Users may not set-up or use any type of e-mailing accounts or applications other than the official district e-mail application. (This includes but is not limited to accounts like Hotmail and Yahoo). Setting up such accounts is strictly prohibited and in direct violation of the user agreement.
30. Staff should not use another employee's computer unless given permission from that party or the district administration.
31. Users should refrain from forwarding mailings that do not directly tie to an employment related function and include music or video clips.

Technology Security and Unauthorized Access

All users shall immediately report any security problems or misuse of the district's technology resources to the building 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 technology resources without authorization are prohibited.
6. The introduction of computer “viruses,” “hacking” tools, or other disruptive/destructive programs into a school computer, the school network, or any external networks are prohibited.
7. Users are not to add, remove or alter computer passwords, security measures, configuration settings or monitoring devices without authorization.

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

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 school computers.**
3. 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.
4. All district employees will abide by state and federal law, Board policies, and district rules when communicating information about personally identifiable students.
5. 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.
6. 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.
7. Before publishing to the Web employees must have signed the Web Publishing Guidelines Agreement and have assured that Consent to Publish Consent form has been signed by the student before posting any student’s work.
8. Any intended damage will be the financial responsibility of the user and accidental damage may be the financial responsibility of the user if good judgement and respect for the equipment was not used.
9. It is the user’s responsibility to report any problems with the computer equipment **immediately**.
10. Users are to utilize the computer/ media equipment for its intended purpose.
11. Software not licensed to the school district should not be used or loaded on any of the districts machines until cleared with the Technology Department to resolve any licensing or compatibility issues.
12. Users should use the computer equipment for work assigned by their administrator unless given permission by their administrator to use the computer for personal use. (The network system administrator can deny a user’s request to utilize the computer for personal use).
13. Computers/media equipment should not be marked on, colored or in any way defaced by a user.
14. Horseplay of any kind is not allowed around any computer/media equipment.
15. Users are not to violate any copyright laws, rules, or regulations when using district computer/media equipment.
16. Users are not to alter or modify any computer/media equipment configuration settings or passwords except file preferences under options or formatting. Users are not to change any setting on software or change any screen settings without the approval of the network administrator or teacher. Any accidental modifications made to the system need to be reported immediately.
17. Accidentally accessing inappropriate sites need to be reported immediately.

18. Users should not assign any unauthorized security protection to any files, programs, or computer/media equipment.
19. Use of obscene, abusive, or otherwise objectionable language, sound, or images in either public or private files or messages is prohibited.
20. Users are solely responsible for the use of their registered account and password. **Only the registered user accesses the assigned account. DO NOT GIVE YOUR PASSWORD TO ANYONE!!**
21. Abusive, physical handling of any equipment by any user is prohibited.
22. Unauthorized copying of any files or media is prohibited. This includes copying or downloading any files.
23. **The use of any e-mail accounts other than the District approved account or Central Web Mail on district computers is prohibited at school.** Students may not set up e-mail profiles under any format.
24. Staff should be familiar with the Approved and Disapproved Downloads List on the District's Web Page.

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.

Violation of any district rules, regulations, or guidelines will result in the loss of the user's privileges to utilize the equipment. **(See Employee Technology Violation document at the end of this document.)**

Access to any one-line information resources, MORE net, Internet, etc. is an unparalleled opportunity to interact with the world at large. This opportunity brings with it a number of responsibilities. The Central R-3 School District provides the opportunity to access electronic on-line resources through MOREnet. In order to have this privilege, you must sign a User Agreement and follow the stated and expressed guidelines.

1. All user 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 system administrator(s) of the computer system 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 or through the computer system.
 - b. Accessing/using another person's registered account, password, files or e-mail accounts.
 - c. Using any defamatory, inaccurate, abusive, obscene, profane, sexually orientated, threatening racially offensive or illegal materials in either public or private files or messages.
 - d. Using an account, 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. **Opening attachments and downloading of materials other than updating anti-virus files must have supervisor permission and may only be saved to a disk.**
 - e. Using an account, 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 to a specified limitation will be posted at the computer sight.
4. The school district reserves the right to inspect any materials stored in files which users have access and will edit or remove any material which the system administrator (s), in its sole discretion, believes may be objectionable.
5. **The school district on-line access is provided primarily for educational purposes under the direction of district staff. Non-educational use may be limited at any time by district staff. Chat lines / Social Networking (or equivalencies) are prohibited.**
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 school district does not warrant that the functions of the system will meet any specific requirements you 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 diskettes, etc.) Sustained or incurred in connection with the use, operation, or inability to use the system.
8. Rules and regulations of system usage will be added and posted to the District Web from time to time by the system administrator(s) reflecting district guidelines. All users are subject to these rules and regulations.
9. File sharing of any type is prohibited.
10. All storage media files brought to school must first be scanned for viruses before using.
11. All users shall immediately report any security problems or misuse of the district's technology resources to an administrator or teacher.

The Central R-III School district on-line access is intended for the exclusive use of its registered users. As a registered user, you are responsible for the appropriate use of your account and the security of your password. 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.

Central R-III Faculty E-mail Policy

E-mail accounts must be used responsibly.

Faculty will only be allowed to use Mozilla Thunderbird or Central Web Mail on District computers. All other types of electronic mail are strictly prohibited and can result in denial of access to the Districts' network.

Faculty 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 ("e-mail") originating from the user's ID or password.
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. **Staff may not send group building or district 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 on-line that are expected in the classroom, and consistent with district policies, regulations and procedures.**
11. Staff may only use the District's established format and centralr3.org e-mail address. 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.
12. Staff should periodically check the Technology link on the district's home page for computer guidelines and approved and disapproved download lists.

Employee Technology Violations

This procedure accompanies the Employee Computer and Internet User Agreement. Each employee is responsible for his/her actions and activities involving school unit computers, networks and Internet Services. The rules do 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 Technology User Agreement.

First Offense: Verbal warning from building administrator.

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

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 Technology 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 schools 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)