Clinton County R-III School District
Acceptable Use Policy

The Clinton County 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 enhancing educational opportunities and achievement of District students. In addition, technology assists with the professional enrichment of the staff and increases engagement of students' families and other patrons of the District, all of which positively impact student achievement.

Definitions

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

Technology Resources – Technologies, devices and services used to access, process, store or communicate information. This definition includes, but is not limited to: computers; modems; printers; scanners; fax machines and transmissions; telephonic equipment; mobile phones; audio-visual equipment; Internet; electronic mail (e-mail); electronic communications devices and services, including wireless access; multi-media resources; hardware; and software. Technology resources may include technologies, devices and services provided to the district by a third party.

User -- any person who is permitted by the District to utilize any portion of the District's technology resources including but not limited to students, employees, School Board members 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 a student or a student's parent/guardian.

Authorized Users

The district's technology resources may be used by authorized students, employees, School Board members and other persons approved by the superintendent or designee, such as consultants, legal counsel and independent contractors. All users must agree to follow the district's policies and procedures and sign or electronically consent to the district's User Agreement prior to accessing or using district technology resources, unless excused by the superintendent or designee.

Use of the district's technology resources is a privilege, not a right. No potential user will be given an ID, password or other access to district technology if he or she is considered a security risk by the superintendent or designee.

User Privacy

A user does not have a legal expectation of privacy in the user's electronic communications or other activities involving the district's technology resources including, but not limited to, voice mail, telecommunications, e-mail and access to the Internet or network drives. By using the district's network and technology resources, all users are consenting to having their electronic communications and all other use monitored by the district. A user ID with e-mail access will only be provided to authorized users on condition that the user consents to interception of or access to all communications accessed, sent, received or stored using district technology.

Electronic communications, downloaded material and all data stored on the district's technology resources, including files deleted from a user's account, may be intercepted, accessed, monitored or searched by district administrators or their designees at any time in the regular course of business. Such access may include, but is not limited to, verifying that users are complying with district policies and rules and investigating potential misconduct. Any such search, access or interception shall comply with all applicable laws. Users are required to return district technology resources to the district upon demand including, but not limited to, mobile phones, laptops and tablets.

Technology Administration

The Board directs the superintendent or designee 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.

Administrators of district technology resources may suspend access to and/or availability of the district's technology resources to diagnose and investigate network problems or potential violations of the law or district policies and procedures. All District technology resources are considered District property. The District may remove, change, or exchange hardware or other technology between buildings, classrooms or users at any time without prior notice. Authorized District personnel may install or remove programs or information, install equipment, upgrade any system or enter any system at any time.

Content Filtering and Monitoring

The District will monitor the on-line 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. The content filter will protect against access to visual depictions that are obscene, harmful to minors, and child pornography. Content filters are not foolproof, and the District cannot guarantee that users will never be able to access offensive materials using District equipment. Evading or disabling, or attempting to evade or disable, a content filter installed by the District is prohibited.

The superintendent, designee or the district's technology administrator may fully or partially disable the district's content filter to enable access for an adult for bona fide research or other lawful purposes. In making decisions to fully or partially disable the district's content filter, the

administrator shall consider whether the use will serve a legitimate educational purpose or otherwise benefit the district.

Online Safety, Security, and Confidentiality

In addition to the use of a content filter, the District will take measures to prevent minors from using District technology to access inappropriate matter or materials harmful to minors on the Internet. Such measures shall include, but are not limited to, supervising and monitoring student technology use, careful planning when using technology in the curriculum, and instruction on appropriate materials. The superintendent, designee and/or the District's technology administrator will develop procedures to provide users guidance on which materials and uses are inappropriate, including network etiquette guidelines.

All minor students will be instructed on safety and security issues, including instruction on the dangers of sharing personal information about themselves or others when using e-mail, social media, chat rooms or other forms of direct electronic communication. Instruction will also address cyberbullying awareness and response and appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms.

This instruction will occur in the District's computer courses, courses in which students are introduced to the computer and the Internet, or courses that use the Internet in instruction. Students are required to follow all District rules when using District technology resources and are prohibited from sharing personal information online unless authorized by the District.

All District employees must abide by state and federal law and Board policies and procedures when using district technology resources to communicate information about personally identifiable students to prevent unlawful disclosure of student information or records.

All users are prohibited from using District technology to gain unauthorized access to a technology system or information; connect to other systems in evasion of the physical limitations of the remote system; copy district files without authorization; interfere with the ability of others to utilize technology; secure a higher level of privilege without authorization; introduce computer viruses, hacking tools, or other disruptive/destructive programs onto District technology; or evade or disable a content filter.

In some instances, the District may outsource institutional and educational functions, such as the collection, maintenance, and storage of student educational records to third parties. These third parties may have access to personal information about students and employees, including but not limited to: names, email addresses, grades, etc. These third parties may also collect personal information directly from students and employees in order to perform the outsourced services. The District will only disclose a student’s personal information in accordance with the Family Educational Rights and Privacy Act (FERPA), and these third parties are bound to comply with FERPA, as well.

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 imprimatur of the District and that are designed to impart particular knowledge or skills to student participants and audiences are considered curricular publications. All curricular publications are subject to reasonable prior restraint, editing and deletion on behalf of the school District for legitimate pedagogical reasons. All other expressive activities involving the District’s technology are subject to reasonable prior restraint and subject matter restrictions as allowed by law and Board policies.

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 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

Use of technology resources in a disruptive, inappropriate or illegal manner impairs the District’s mission, squanders resources and shall not be tolerated. Therefore, a consistently high level of personal responsibility is expected of all users granted access to the District’s technology resources. Any violation of District policies or procedures regarding technology usage may result in temporary, long-term or permanent suspension of user privileges. User privileges may be suspended pending investigation into the use of the District’s technology resources.

Employees may be disciplined or terminated, and students suspended or expelled, for violating the District’s technology policies and procedures. Any attempted violation of the District's technology policies or procedures, regardless of the success or failure of the attempt, may result in the same discipline or suspension of privileges as that of an actual violation. The District will cooperate with law enforcement in investigating any unlawful use of the District's technology resources.

Damages

All damages incurred by the District due to a user’s intentional or negligent misuse of the District’s technology resources, including 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.

The District is not responsible for loss of data, delays, non-deliveries, misdeliveries or service interruptions. The District does not endorse the content nor guarantee the accuracy or quality of information obtained from using its technology resources.

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 filed 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 the 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 form 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 investigation and prosecution of persons using District technology in violation of 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. The District prohibits the use of District technology resources to access, view, or disseminate information that constitutes insulting or fighting words, the very expression of which injures or harasses other people (e.g. threats of violence, defamation of character or of a person's race, religion, or ethnic origin); presents a clear and present likelihood that, because of their content or their manner of distribution, 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 policies or procedure is prohibited.
14. Any use that violates any person's rights under applicable laws, specifically use that has the purpose or effect of discriminating or harassing any person 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 is strictly prohibited.
15. The District prohibits unauthorized intentional or negligent action that damages or disrupts technology, alters its normal performance, or causes it to malfunction. The District will hold users responsible for such damage and will seek both criminal and civil remedies, as necessary.
16. Users may 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 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 District so that any licensing or compatibility issues have been resolved.

17. At no time will the District's 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. 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 form the equipment supervisor.
25. Students and community users may only access computer programs that have been assigned by the supervisor.
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. Students 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. Students 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. Students may not set up or use any type of e-mailing accounts or applications not approved by the District.
30. Students 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. Students should use computer/media equipment for school/class work assigned by their instructor unless given permission by their instructor to use 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. The use of student e-mail at school is limited to the District assigned account for the Clinton County R-III domain. Students may not set up e-mail accounts under any other format. 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 District.

Technology Security and Unauthorized Access

1. All users shall immediately report any security problems or misuse of the District's technology resources to a teacher or administrator.
2. Use of District technology resources in attempting to gain or gaining unauthorized access to any technology system or the files of another is prohibited.
3. Use of District technology to connect to other systems, in evasion of the physical limitations of the remote system, is prohibited.
4. The unauthorized copying of system files is prohibited.
5. Intentional or negligent attempts, whether successful or unsuccessful, to interfere with the ability of others to utilize any District technology are prohibited.
6. Any attempts to secure a higher level of privilege on the District's technology resources without authorization are prohibited.
7. 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.
8. 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

Curricular or noncurricular publications distributed using district technology will comply with the law and Board policies on confidentiality.

All district employees will abide by state and federal law, Board policies and district rules when using district technology resources to communicate information about personally identifiable students. Employees will take precautions to prevent negligent disclosure of student information or student records.

All students will be instructed on the dangers of sharing personal information about themselves or others over the Internet and are prohibited from sharing such information unless authorized by the district. Student users shall not agree to meet with someone they have met online without parental approval and must promptly disclose to a teacher or another district employee any message the user receives that is inappropriate or makes the user feel uncomfortable.

1. Student 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.
2. Student users shall not agree to meet with someone they have met on-line without parental approval.

3. 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.
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 District 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. 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 Student User Agreement Violation section.).

Student Use of Personal Electronic Devices for Learning

Utilization of personal electronic devices for learning/educational purposes 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 including, but not limited to, suspension of access as described in the Student User Agreement Violation section.

Further, users understand and agree to the following:

1. Permission must be granted from individual classroom teachers prior to using any personal electronic devise during classroom instructional time.

2. Personal electronic devices used during the school day shall only be used for appropriate educational purposes and be consistent with the educational objectives of the District.
3. The District assumes no liability for lost, stolen, damaged or misplaced devices, including those that have been confiscated by District personnel.
4. The District may examine personal electronic devices to the extent allowed by law.
5. Any data plan associated with user's personal electronic device shall be disabled during the school day, and users agree to only use the District's network during the school day.
6. 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 damage.
7. 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.
8. 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.

Student in Violation of User Agreement

Students in Violation of this User Agreement will be subject to discipline as outlined in Board Policy and Regulation JG and JG-R1, which can be found on the District's website.