CAMDENTON R-III STUDENT TECHNOLOGY ACCEPTABLE USE POLICIES

2017-2018

Contents

1.) INTERNET SAFETY POLICY

Introduction

It is the policy of the District to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act (CIPPA)[Pub. L. No. 106-554 and 47 USC 254(h)].

Access to Inappropriate Material

To the extent practical, technology protection measures shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information. Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.

Internet Safety Training

In compliance with the Children's Internet Protection Act, each year, all District students will receive internet safety training which will educate students about appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms, and cyberbullying awareness and response. Such training will include Internet, cell phones, text messages, chat rooms, email and instant messaging programs. (See also – State Mandated Curriculum – Human Sexuality - IGAEB).

Inappropriate Network Usage

To the extent practical, steps shall be taken to promote the safety and security of users of the District's online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications. Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called "hacking," and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

Supervision and Monitoring

It shall be the responsibility of all District employees to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet protection Act. Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Camdenton R-III School District Superintendent or designated representatives.

2.) INTERNET USAGE POLICY

Personal Responsibility

Access to electronic research requires students to maintain consistently high levels of personal responsibility. The existing rules found in the District's Behavioral Expectations policy (JG) clearly apply to students conducting electronic research or communication.

One fundamental need for acceptable student use of District electronic resources is respect for, and protection of, password/account code security, as well as restricted databases files, and information banks. Personal passwords/account codes may be created to protect students utilizing electronic resources to conduct research or complete work.

These passwords/account codes shall not be shared with others; nor shall students use another party's password except in the authorized maintenance and monitoring of the network. The maintenance of strict control of passwords/account codes protects students from wrongful accusation of misuse of electronic resources or violation of District policy, state or federal law. Students who misuse electronic resources or who violate laws will be disciplined at a level appropriate to the seriousness of the misuse.

Acceptable Use

The use of the District technology and electronic resources is a privilege, which may be revoked at any time. Staff and students are only allowed to conduct electronic network-based activities which are classroom or workplace related. Behaviors which shall result in revocation of access shall include, but will not be limited to: damage to or theft of system hardware or software; alteration of system hardware or software; placement of unlawful information, computer viruses or harmful programs on, or through the computer system; entry into restricted information on systems or network files in violation of password/account code restrictions; violation of other users' rights to privacy; unauthorized disclosure, use or dissemination of personal information regarding minors; using another person's name/password/account to send or receive messages on the network; sending or receiving personal messages on the network; and use of the network for personal gain, commercial purposes, or to engage in political activity.

Students may not claim personal copyright privileges over files, data or materials developed in the scope of their employment, nor may students use copyrighted materials without the permission of the copyright holder. The Internet allows access to a wide variety of media. Even though it is possible to download most of these materials, students and staff shall not create or maintain archival copies of these materials unless the source indicates that the materials are in the public domain.

Access to electronic mail (E-mail) is a privilege and designed to assist students in the acquisition of knowledge and in efficiently communicating with others. The District E-mail system is designed solely for educational and work related purposes. ***E-mail files are subject to review by District and school personnel***. Chain letters, "chat rooms" or Multiple User Dimensions (MUDs) are not allowed, with the exception of those bulletin boards or "chat" groups that are created by teachers for specific instructional purposes.

Students who engage in "hacking" are subject to loss of privileges and District discipline, as well as the enforcement of any District policy, state and/or federal laws that may have been violated. Hacking may

be described as the unauthorized review, duplication, dissemination, removal, damage, or alteration of files, passwords, computer systems, or programs, or other property of the District, a business, or any other governmental agency obtained through unauthorized means.

To the maximum extent permitted by law, students are not permitted to obtain, download, view or otherwise gain access to "inappropriate matter" which includes materials that may be deemed inappropriate to minors, unlawful, abusive, obscene, pornographic, descriptive of destructive devices, or otherwise objectionable under current District policy or legal definitions. Similarly, the use of any District computer to access sites which allow the user to conceal their objective of accessing inappropriate material is not permitted.

The District and school administration reserve the right to remove files, limit or deny access, and refer staff or students violating the Board policy to appropriate authorities or for other disciplinary action.

Internet Access

In compliance with the Children's Internet Protection Act ("CIPA"), 47 U.S.C. § 254, the District uses technological devices designed to filter and block the use of any District computer with Internet access to retrieve or transmit any visual depictions that are obscene, child pornography, or "harmful to minors" as defined by CIPA and material which is otherwise inappropriate for District students.

Due to the dynamic nature of the Internet, sometimes Internet websites and web material that do not fall into these categories are blocked by the filter. In the event that a District student feels that a website or web content has been improperly blocked by the District's filter and this website or web content is appropriate for access by District students, the process described below should be followed:

1. Follow the process prompted by the District's filtering software (or to remain anonymous, log in under log in name: 123anonymous) and submit an electronic request for access to a website, or:
2. Submit a request, whether anonymous or otherwise, to the District's Superintendent/the Superintendent's designee.
3. Requests for access shall be granted or denied within three days. If a request was submitted anonymously, persons should either attempt to access the website requested after three days or log back in at 123anonymous to see the status of the request.
4. Appeal of the decision to grant or deny access to a website may be made in writing to the Board of Education. Persons who wish to remain anonymous may mail an anonymous request for review to the Board of Education at the School District's Central Office, stating the website that they would like to access and providing any additional detail the person wishes to disclose.
5. In case of an appeal, the Board of Education will review the contested material and make a determination.
6. Material subject to the complaint will not be unblocked pending this review process.

In the event that a District student feels that a website or web content that is available to District students through District Internet access is obscene, child pornography, or "harmful to minors" as defined by CIPA or material which is otherwise inappropriate for District students, the process described set forth in IIAC-R1.

Adult users of a District computer with Internet access may request that the "technology protection measures" be temporarily disabled by the chief building administrator of the building in which the computer is located for lawful purposes not otherwise inconsistent with this Policy.

Privileges

The use of District technology and electronic resources is a privilege, not a right, and inappropriate use will result in the cancellation of those privileges. All staff members and students who receive a password/account code will participate in an orientation or training course regarding proper behavior and use of the network. The password/account code may be suspended or closed upon the finding of user misuse of the technology system or its resources.

Network Etiquette and Privacy

Students are expected to abide by the generally accepted rules of electronic network etiquette. These include, but are not limited to, the following:

1. System users are expected to be polite. They may not send abusive, insulting, harassing, or threatening messages to others.
2. System users are expected to use appropriate language; language that uses vulgarities or obscenities, libels others, or uses other inappropriate references is prohibited.
3. System users may not reveal their personal addresses, their telephone numbers or the addresses or telephone numbers of students, employees, or other individuals during E-mail transmissions.
4. System users may not use the District's electronic network in such a manner that would damage, disrupt, or prohibit the use of the network by other users.
5. System users should assume that all communications and information is public when transmitted via the network and may be viewed by other users. The system administrators may access and read E-mail on a random basis.
6. Use of the District's electronic network for unlawful purposes will not be tolerated and is prohibited.

Children's Online Privacy Protection (COPPA)

COPPA applies to commercial companies and limits their ability to collect personal information from children under 13. These programs must provide parental notification and obtain parental consent before collecting personal information from children under the age of 13. The law permits the District to consent to the collection of personal information on behalf of all of its students, thereby eliminating the need for individual parental consent given directly to the third party operator. The Technology User Consent Form allows the District to act as an agent for parents in the collection of personal information within the school context. The Technology User Consent Form constitutes consent for your student and/or the district to provide personal information to third party operators. No personal student information is collected for commercial purposes. The District's use of student personal Information is solely for education purposes. For more information on COPPA, please visit:
https://www.ftc.gov/tips-advice/business-center/guidance/complyingcoppa-frequently-asked-questions.

Family Educational Rights and Privacy Act (FERPA)

FERPA protects the privacy of student education records from unauthorized disclosure. FERPA gives parents the right to access their children's education records and the right to consent to disclosure of personally identifiable information from the records. Under FERPA, schools may disclose directory information (see - JO). The term "education records" is defined as those records that contain information directly related to a student and which are maintained by an educational agency. FERPA allows "school officials" to obtain access to personally identifiable information contained in education records provided the school has determined that the official has a "legitimate educational interest" in the information.

Services

While the District is providing access to electronic resources, it makes no warranties, whether expressed or implied, for these services. The District may not be held responsible for any damages including loss of data as a result of delays, non-delivery or service interruptions caused by the information system or the user's errors or omissions. The use or distribution of any information that is obtained through the information system is at the user's own risk. The District specifically denies any responsibility for the accuracy of information obtained through Internet services.

Security

The Board recognizes that security on the District's electronic network is an extremely high priority. Security poses challenges for collective and individual users. Any intrusion into secure areas by those not permitted such privileges creates a risk for all users of the information system.

The account codes/passwords provided to each user are intended for the exclusive use of that person. Any problems, which arise from the user sharing his/her account code/password, are the responsibility of the account holder. Any misuse may result in the suspension or revocation of account privileges. The use of an account by someone other than the registered holder will be grounds for loss of access privileges to the information system.

Users are required to report immediately any abnormality in the system as soon as they observe it. Abnormalities should be reported to the classroom teacher or system administrator.

The District shall use filtering, blocking or other technology to protect students and staff from accessing internet sites that contain visual depictions that are obscene, child pornography or harmful to minors. The District shall comply with the applicable provisions of the Children's Internet Protection Act (CIPA), and the Neighborhood Internet Protection Act (NCIPA).

Vandalism of the Electronic Network or Technology System

Vandalism is defined as any malicious attempt to alter, harm, or destroy equipment or data of another user, the District information service, or the other networks that are connected to the Internet. This includes, but is not limited to the uploading or the creation of computer viruses, the alteration of data, or the theft of restricted information. Any vandalism of the District electronic network or technology system will result in the immediate loss of computer service, disciplinary action and, if appropriate, referral to law enforcement officials.

Consequences

The consequences for violating the District's Acceptable Use Policy include, but are not limited to, one or more of the following:

1. Suspension of District Network privileges;
2. Revocation of Network privileges;
3. Suspension of Internet access;
4. Revocation of Internet access;
5. Suspension of computer access;
6. Revocation of computer access;
7. School suspension;

8. Expulsion;

3.) STUDENT USE OF PERSONAL ELECTRONIC DEVICES FOR INSTRUCTIONAL PURPOSES

The Camdenton R-III School District recognizes that students increasingly have access to and are using personal electronic devices for many purposes, including educational purposes. The Board authorizes the superintendent and/or designated authority and building principals to designate classes, grade levels and/or buildings where teachers are encouraged to utilize and incorporate personal electronic devices into their instruction and lesson plans in accordance with this policy. Teachers who incorporate such technology into their classrooms shall, with the assistance of the principal or designee, make accommodations for those students who do not have access to personal electronic devices. No student shall be penalized in any fashion for failure to own or have access to personal electronic devices.

Definitions

District Networks – Include both wired and wireless networks maintained by the district.
Personal Electronic Devices – Are communication devices with voice, text, data, and/or navigation capabilities that are able to access the Internet, transmit phone calls, text messages, e-mail messages or video communications, perform word processing and other computer and online applications, and/or provide location information. These include devices which are capable of electronically communicating, sending, receiving, storing, recording, producing and/or displaying information and data. These devices include, but are not limited to, electronic communication equipment such as laptops, portable media players, mobile phones, smart phones, tablet computers and video game devices owned by a student or a student's parent/guardian.

Acceptable Use

Possession or use of any personal electronic device on district property is a privilege, and students who fail to abide by this policy may forfeit this privilege.

When approved by the building principal and/or designated authority, students will be allowed to bring personal electronic devices to school for use during the school day in the designated classrooms. Each building administrator, under the direction of the superintendent or designee, shall determine the appropriate areas of the school where students may use personal electronic devices and the extent to which such devices will be incorporated into the classroom curriculum.

Students may use personal electronic devices during the school day only if the student and parents/guardians sign and agree to the terms of the district's personal electronic devices agreement and the district's technology usage agreements unless excused by the superintendent or designee. Students shall only access the Internet through district-provided networks during the school day. Student devices with a data plan through the students or parent's/guardian's mobile provider must have the external network turned off when on school premises during the school day. The district will utilize a technology protection measure, such as a filter, on all district networks. Students shall not bypass or attempt to bypass the district's networks through any means.

Possession or use of personal electronic devices must not in any way disrupt the educational process in the school district, endanger the health or safety of the student or any other person in the district, invade the rights of others at school or involve illegal or prohibited conduct.

All use of personal electronic devices during the school day shall be for appropriate educational purposes only, not for personal use, and shall be consistent with the educational objectives of the district. Students

using personal electronic devices must follow the same rules that apply to the use of district-provided technology. The district may examine the student's device to the extent allowed by law. The district administration may involve law enforcement if the district has reasonable suspicion that the device has been used for an illegal purpose or for a purpose that causes harm to others.

The district shall not be liable for theft, loss, damage, misuse or unauthorized use of any personal electronic communication device brought to school or school-sponsored programs/activities by a student.

No school funds shall be used to purchase programs or applications to be downloaded on any personally owned communication device utilized by students unless approved by designee.

Failure to abide by this policy shall subject the student to disciplinary action as outlined elsewhere in Board policy.

Delegation of Responsibility

The superintendent or designee is granted the authority to create and enforce regulation(s), rules, procedures and forms to accompany this policy.

He/she shall annually notify students, parents/guardians, employees and guests about the use of personal electronic communication devices by publishing the policy on the district's website and ensuring it is included in student handbooks, posted notices and/or any other methods.

The superintendent working with technology and/or designee is responsible for annual training of administrators and employees who are responsible for the use, supervision, discipline, investigation, confiscation, searching and/or other matters involving students' use of electronic communication devices, including personal electronic communication devices.

Guidelines

In accordance with this policy, personal electronic communication devices may be used in authorized areas or as determined by the administration as follows:

1. For educational and instructional purposes.
2. When the educational, safety, emergency, medical or security use of the device is approved by the teacher/facilitator, program supervisor or designee.

In accordance with this policy, personal electronic communication devices may not be used in unauthorized areas or as determined by the administration as follows:

1. Devices that control/interfere with the operation of the buildings' systems, facilities and infrastructure or digital network. No exception or permission may be authorized for students to possess or use such devices.
2. During tests, examinations and/or assessments unless the teacher/facilitator authorizes such use. When personal electronic communication devices are prohibited for use on tests, they must be stored in closed items, such as book bags or purses, and may not be visible or turned on.
3. To cheat, engage in unethical conduct or threaten academic integrity.
4. To access and/or view Internet websites that are blocked by the district's filtering system.

5. To take action that would invade the privacy rights of any student, violate the rights of any student, or harass, threaten, intimidate, promote or engage in violence, bully or cyberbully any student.
6. In locker rooms, bathrooms, dressing rooms or any other changing area.
7. To create, send, share, view or disseminate sexually explicit, obscene, pornographic, child pornographic or lewd images or video content, as such acts may be a crime under state and/or federal law.
8. To disrupt the educational or learning environment.

Devices that violate this policy and/or other relevant district policies shall be confiscated and retained by the building administrator. The confiscated device shall not be returned until a conference is held with the parent/guardian. Violations of this policy should be reported to the assistant superintendent in charge of technology.

4.) TECHNOLOGY USAGE

The Camdenton R-III School District's technology exists for the purpose of enhancing the educational opportunities and achievement of district students. Research shows that students who have access to technology improve achievement. 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. The district will periodically conduct a technology census to ensure that instructional resources and equipment that support and extend the curriculum are readily available to teachers and students.

The purpose of this policy is to facilitate access to district technology and to create a safe environment in which to use that technology. Because technology changes rapidly and students need immediate guidance, the superintendent or designee is directed to create procedures to implement this policy and to regularly review those procedures to ensure they are current.

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; personal digital assistants (PDAs); 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 that would allow a user access to the district's technology resources or to any program including, but not limited to, e-mail and Internet access.

Password – A unique word, phrase or combination of alphabetic, numeric and non-alphanumeric characters used to authenticate a user ID as belonging to a user.

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 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 information retained on 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 online activities and operate a technology protection measure ("content filter") on the network and all district technology with Internet access, as required by law. In accordance with law, the content filter will be used to protect against access to visual depictions that are obscene or harmful to

minors or are child pornography. 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 room.

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.

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 webpage will provide information about the school 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.

Violations of Technology Usage Policies and Procedures

Use of technology resources in a disruptive, wasteful, 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.

Students may be 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 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/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, miss-deliveries or service interruptions. The district does not endorse the content nor guarantee the accuracy or quality of information obtained using the district's technology resources.

Student Users

All student users and their parents/guardians must sign or electronically consent to the district's User Agreement prior to accessing or using district technology resources, unless otherwise excused by this

policy or the superintendent or designee. Students who are 18 or who are otherwise able to enter into an enforceable contract may sign or consent to the User Agreement without additional signatures.

General Rules and Responsibilities

The following rules and responsibilities will apply to all users of the district's technology resources:

1. Applying for a user ID under false pretenses or using another person's ID or password is prohibited.
2. Sharing user IDs or passwords with others is prohibited, and users will be responsible for any actions taken by those using the ID or password. A user will not be responsible for theft of passwords and IDs, but may be responsible if the theft was the result of user negligence.
3. Deleting, examining, copying or modifying files or data belonging to other users without their prior consent is prohibited.
4. Mass consumption of technology resources that inhibits use by others is prohibited.
5. Use of district technology for soliciting, advertising, fundraising, commercial purposes or financial gain is prohibited, unless authorized by the district. Use of district technology resources to advocate, support or oppose any ballot measure or candidate for public office is prohibited.
6. 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.
7. 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.
8. The district prohibits the use of district technology resources to access, view or disseminate information that is pornographic, obscene, child pornography, harmful to minors, obscene to minors, libelous, or pervasively indecent or vulgar.
9. 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.
10. 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, they 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 district policies and procedures.
11. The district prohibits any use that violates any person's rights under applicable laws, and specifically prohibits any use that has the purpose or effect of discriminating against or harassing any person on the basis of race, color, religion, sex, national origin, ancestry, disability, age, genetic information, pregnancy or use of leave protected by the Family and Medical Leave Act (FMLA).
12. The district prohibits any 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.

13. Users may only install and use properly licensed software and audio or video media purchased by the district or approved for use by the district and users must have written permission from the superintendent or designee for such installation and use. 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.
14. At no time will district technology or software be removed from district premises, unless authorized by the district.
15. All users will use the district's property as it was intended. Technology resources will not be moved or relocated without permission from the superintendent or designee. All users will be held accountable for any damage they cause to district technology resources.

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. Users will be granted access privileges to district technology resources as determined appropriate by the superintendent or designee. Any attempt to secure a higher level of privilege without authorization is prohibited.
7. The introduction of computer viruses, hacking tools or other disruptive or destructive programs into a district computer, network or any external networks is prohibited.

Online Safety and Confidentiality

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.

Electronic Mail and Messaging

A user is responsible for all e-mail and other electronic messages originating from the user's e-mail or other electronic messaging accounts.

1. Forgery or attempted forgery of electronic messages is illegal and prohibited.
2. Unauthorized attempts to read, delete, copy or modify electronic messages of other users are prohibited.
3. Users are prohibited from sending unsolicited mass e-mail or other electronic messages. The district considers more than one address per message, per day a violation, unless the communication is a necessary, employment-related function or an authorized publication.
4. When communicating electronically, all users must comply with district policies, regulations and procedures and adhere to the same standards expected in the classroom.
5. Users must obtain permission from the superintendent or designee before sending any districtwide electronic messages.

Waiver

Any user who believes he or she has a legitimate educational purpose for using the district's technology in a manner that may violate any of the district's policies, regulations or procedures may request a waiver from the building principal, superintendent or their designees. In making the decision to grant a waiver to a student, the administrator shall consider the purpose, age, maturity and level of supervision involved.

5.) GOOGLE APPS FOR EDUCATION (G Suite for Education)

The Camdenton R-III School District utilizes Google Apps for Education (G Suite for Education) for students, teachers, and staff. As with any educational endeavor, a strong partnership with families is essential to a successful experience. With this letter we are sharing information regarding the use of Google Apps for Education in the Cedarburg School District and are requesting your parental permission for your student to use Google Apps.

What does Google Offer?

The following core services are available to each student and hosted by Google as part of Camdenton R-III School District's online presence in Google Apps for Education: Gmail, Calendar, Classroom, Contacts, Drive, Docs, Forms, Groups, Sheets, Sites, Slides, Talk/Hangouts and Vault

Information about GAFE can be found here
http://www.google.com/enterprise/apps/education/benefits.htm

Using these tools, students collaboratively create, edit, and share files and websites for school related projects and communicate via email with other students and teachers. These services are entirely online and available 24/7 from any Internet-connected computer. Examples of student use include showcasing class projects, building an electronic portfolio of school learning experiences, and working in small groups on presentations to share with others.

Google Apps for Education use in the Camdenton R-III School District is governed by federal laws and local board policies including:

Family Educational Rights and Privacy Act (FERPA)
FERPA protects the privacy of student education records and gives parents the rights to review student records. Under FERPA, schools may disclose directory information but parents may request the school not disclose this information. Parents are provided the opportunity annually to opt out of disclosing their student's directory information on the District's Enrollment Form. --FERPA – http://www.ed.gov/policy/gen/guid/fpco/ferpa

Children's Online Privacy Protection Act (COPPA)
COPPA applies to commercial companies and limits their ability to collect personal information from children under 13. By default, advertising is turned off for Cedarburg School District's presence in Google Apps for Education. No personal student information is collected by Google for commercial purposes. This permission form allows the school to act as an agent for parents in the collection of information within the school context. The school's use of student information is solely for education purposes. Student information that is "collected" by Google is described as (projects, documents, email, files, username and password). --COPPA – http://www.ftc.gov/privacy/coppafaqs.shtm

What should I be aware of?

- Unlike many other web services GAFE acknowledges its users as the owners of content they produce and store
- GAFE does not share any data or user information with any other party unlike other Google products such as Gmail.
- Your child will be provided an email address as part of the GAFE package.
- Students in grades K-6 can ONLY send or receive emails within the district's domain; that is emails ending with camdentonschools.org. Students in grades 7-10 will be able to email within our domain and with accounts ending in .edu to allow collaboration with educational sites. Student email accounts for grades 11 and 12 will be open.

GAFE terms of service can be read here: http://www.google.com/apps/intl/en-GB/terms/education_terms.htm

For additional privacy and security information see the following links:

https://edu.google.com/trust/ (Google for Education Trust Page)

https://gsuite.google.com/terms/education_privacy.html (G Suite for Education Privacy Statement)

https://www.google.com/intl/en/policies/technologies/product-privacy/ (Product Privacy Guide)

What rules and practices are in place to keep students safe?

Email messages sent from students using the provided email system are required to adhere to strict District policies. All email account users should be aware of the following:
Camdenton R-III School District may monitor all inbound and outbound emails for viruses, profanity, offensive language, racist and sexual comments, virus hoaxes, chain-mail, and known spam mailers. You should not assume that your District GAFE account is private. Camdenton R-III School District reserves the right to intercept, store, archive, delete, or view such emails for security purposes; and, where necessary, investigate inappropriate subject matter by the parties involved.

Student expectations include the following:

- Students will use this email account for the purpose outlined in the course expectations.
- Students will exhibit respect and courtesy at all times when using their email account.
- Students will understand that this email account can and will be monitored for inappropriate usage.

Any violation of the Acceptable Use Agreement will result in disciplinary action based on the policies of the school and district. These supplement the school district's Policy for Acceptable Use of Technology Resources as stated in each school's student handbooks. Students will not use this email account to send or receive derogatory subject matter. Students under age 13 ordinarily need parent permission to have email accounts. However, COPPA (Child Online Privacy Protection Act) allows schools to act as the parents' agent and approve *Google Apps for Education* accounts on their behalf. To be COPPA compliant, we have an opt out process. If you would like to discuss this, please refer to this form on the district technology page located on the www.camdentonschools.org website.

We want you to be involved with your student's education. We encourage you to log into *Google Apps for Education* with your student to see what it's all about! If you wish to discuss how *Google Apps for Education* is used at our schools, please contact your child's teacher, building principal, or another school representative.

6.) OTHER THIRD PARTY SOFTWARE APPLICATIONS AND WEB-BASED SERVICES

The District utilizes computer software applications and web-based services operated not by the District but by third parties. These include Google Apps for Education (see 5 above), RAZ-kids, Destiny, Study Island, i-Ready, Clever, Canvas, and similar educational programs. A complete list of the programs with the privacy policy for each can be found on the district website. In order for students to use these services, certain personal information - generally the student's name and email address - must be provided to the third party operator.Technology use in the District is governed by federal laws and regulations including: Children's Online Privacy Protection Act (COPPA) and the Family Educational Rights and Privacy Act (FERPA). These laws and regulation descriptions were referred to earlier in this document.

7.) PARENT CONSENT PAGES

Camdenton R-III Student Technology Acceptable Use Policies
(Student User Agreement)

I have read ALL Camdenton R-III Student Technology Acceptable Use policies and procedures (sections 1 - 6) in this document and agree to abide by their provisions. I understand that violation 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 suspension or expulsion from school.

I understand that my use of the Camdenton R-3 School District technology resources is not private and that the school district may monitor my electronic communications and all other use of district technology resources.

I consent to district interception of or access to all of my electronic communications using district technology resources as well as downloaded material and all data I store on the Camdenton R-3 School District technology resources, including deleted files, pursuant to state and federal law, even if the Camdenton R-3 School District technology resources are accessed remotely.

I understand that possession and use of any personal electronic device is a privilege, not a right, and that I may forfeit this privilege by failing to abide by any terms of this policy. I understand that violation of these provisions may result in disciplinary action taken against me including, but not limited to, suspension of my access to the district's networks and suspension or expulsion from school.

Further, I understand and agree to the following:

1. All use of personal electronic devices during the school day shall be for appropriate educational purposes only and shall be consistent with the educational objectives of the district.

2. The district may examine my device to the extent allowed by law.

3. The district assumes no liability for lost, stolen, damaged or misplaced devices, including those that have been confiscated by district personnel.

4. Any data plan associated with my personal electronic device shall be disabled during the school day, and I hereby agree to only use the district's networks during the school day.

5. The district is not responsible for any loss of information that may arise from the use of the district's networks or any resulting loss, injury or damages.

6. The district will not be responsible for technological support of the personal electronic devices, and I am required to make sure that my devices are free from viruses before bringing them to school.

I understand that this consent form will be effective for the duration of my attendance in the district unless revoked or changed by the district or me.

Name of Student: (Print) _____ Date: _____

Building: _____ Grade: _____

Parent/Guardian Consent: _____ Date: _____

Camdenton R-III School District
Google Apps for Education Parent Permission Form

By signing below, I confirm that I have read and understand the following:

Under FERPA and corresponding Missouri law, a student's education records are protected from disclosure to third parties. With regards to COPPA, I understand that my student's education records (projects, documents, email, files, username and password) stored in Google Apps for Education may be accessible to persons acting on behalf of Google by virtue of this online environment. This does not include any student demographic or grade information stored on the Camdenton R-3 School Network. I also understand that my student's use of Google Apps for Education is governed by all Camdenton R-III School District policies for Student Acceptable Use of Technology.

I have read and understand section 5.) above ("Google Apps for Education").

My signature below confirms my consent to allow my student's education records (projects, documents, email, files, username and password) to be stored by Google. I understand that I may ask for my child's account to be removed at any time.

I give permission for my child to be assigned a full Camdenton R-III School District Apps for Education account. This means my child will receive an email (Gmail) account (as referenced in the Google Apps for Education Policy above) and access to all core (see section 5) G Suite for Education services.

Name of Student: (Print) _____ Date: _____

Building: _____ Grade: _____

Parent/Guardian Consent: _____ Date: _____