



INTERNET ACCESS AND USAGE

A major goal of the Rockwood School District is to promote educational excellence by facilitating resource sharing, innovation, and communications by providing access to electronic-based information technology, including electronic mail (email) and internet access to students, staff, teachers and administrators in the district. Technology, used as an educational tool, can enhance student learning and expand the scope of instruction in many innovative ways. The internet, email and other digital resources are to be used in a manner that is consistent with the district's standards of conduct and as part of the normal execution of the employee's or student's responsibilities. Use of these technology resources in a disruptive, inappropriate or illegal manner impairs the district's mission, wastes resources and will not be tolerated. The use of the district's technology and electronic resources is a privilege which may be revoked at any time.

District technology resources are defined as those technologies, devices and services used to access, process, store, or communicate information. Examples of district technology resources include, but are not limited to: computers; modems; printers; scanners; fax machines and transmissions; telephonic equipment; mobile phones; audio-visual equipment; internet; electronic mail (e-mail); electronic communication devices and services, including wireless access; multimedia resources; hardware; and software. Technology resources may include technologies, devices and services provided to the district by a third party.

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.

All Rockwood School District computer users should be aware of the following:

- All users granted access to the district's technology resources are expected to maintain a high level of professional and personal responsibility. Employee handbooks and the Behavioral Expectations policy contain the existing rules and clearly apply to students and employees conducting electronic research or communication.
- Any use that jeopardizes the safety, security or usefulness of the district's technology resources or interferes with the effective and professional performance of the employee's job is considered unreasonable. Unless authorized by the employee's supervisor, employees may not access, view, display, store, print or disseminate information using district technology resources that students or other users could not access, view, display, store, print or disseminate.
- Use of the district's internet, email and other digital resources are strictly intended to conduct and complete the duties assigned to the employee or student.
- Social media accounts should be used exclusively for the district and classroom-related work and communication. District employees may not use district accounts for personal use.
- If an employee witnesses a violation of the internet usage regulation, the employee shall report the incident to their supervisor.
- If a student witnesses a violation of the internet usage regulation, the student shall report the incident to the building principal.

- The Rockwood School District filters internet content. This limits the internet sites that can be accessed by all network computer users including students, teachers, administrators, other staff and visitors. Because e-rate funds are used to provide the district's Internet access, the district must comply with the Children's Internet Protection Act (CIPA) by using a CIPA compliant content filtering system. These limits do not provide a foolproof filter to limit access to controversial material and the Rockwood School District will not be liable for any damages as a result of accessing objectionable material.
- All electronic-based information technology activity, including email and internet searches, are subject to monitoring by the Rockwood School District technology staff and students and employees have no right of privacy in any such data. Any discovered computer activity including, but not limited to an email message or internet search that deals with inappropriate or illegal activities will be reported to the appropriate authority. Personal information and personal data files from individuals suspected of committing a crime may also be turned over to investigators by administrators of the district. The district will comply with any search warrants including those issued under the USA Patriot Act of 2001 which targets terrorist offenses.
- Passwords are not to be used by unauthorized individuals. Individuals provided with system passwords will assume responsibility for the proper use of those passwords. If a student or staff member feels that there is a security problem on the network, misuse of a district password, or a compromised password should report the matter immediately to the Technology Help Desk.
- All users must abide by existing state and federal laws regarding electronic communication, including accessing information without authorization, sharing passwords, or causing a system to malfunction. All users must abide by all Rockwood School District regulations and policies governing electronic data and electronic mail (email) retention.
- All digital applications and locally installed software used by district employees and students must be approved by the Technology Department. Student projects posted on district servers and/or digital resources must follow district guidelines for acceptable content. District policies and regulations on student publications will also extend to school-sponsored web publications.
- Students or employees who engage in investigatory activities commonly described as "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.
- Students and employees are expected to abide by generally accepted rules of electronic network etiquette: be polite in all communications; use appropriate language; do not share personal information other than as required by the district; do not damage, disrupt or prohibit use of the network by others; assume all transmissions via the network are public.
- Consequences for violating the district's Internet Usage Policy and Regulation will be enforced and include, but are not limited to: suspension of district network privileges; revocation of network privileges; suspension of computer and Internet access; revocation of computer and Internet access; school suspension; expulsion; employee disciplinary action up to and including dismissal; legal action to recover financial damages; criminal legal action.



INTERNET ACCESS AND USAGE

The following activities are among those not allowed on Rockwood School District's network and constitute a violation of the Rockwood School District Policy/Regulation 6321:

- Sharing confidential information about students or employees other than in the discharge of professional duties
- Sharing your password with other users
- Accessing harmful, abusive, obscene, pornographic, descriptions of destructive devices, hateful, unlawful or otherwise objectionable material under current district policy or legal definitions
- Using obscene, vulgar, harassing or libelous language in electronic data files or email
- Harassing, threatening, insulting or harming others in any way via email, electronic data or other network access
- Attempting to compromise security systems by any means or technology
- Using or capturing other users' passwords
- Attempting to access without consent, destroy or damage the data files of others
- Running packet capture or network sniffer programs or systems without approval from the Technology Department
- Running network discovery or monitoring systems without approval from the Technology Department
- Intentionally distributing a computer virus, Trojan horse or any other type of malware program on district computers or network devices
- Downloading, filing, relaying or running any game or entertainment software or game server software, including games that run inside of web browsers except for specific instructional purposes
- Running programs designed to disrupt the network or create a denial of service of any district system or external system
- Running peer to peer file sharing systems without approval from the Technology Department
- Bypassing or defeating the web content filtering system without approval from the Technology Department
- Intentionally running programs that may "crash" or render the network and/or its components unreliable
- Utilizing or attempting to use any wireless personal computing device to connect to Rockwood School District's network without prior approval for purposes other than approved, including but not limited to downloading music, videos, or other data files
- Utilizing or attempting to use any wireless personal computing device to disrupt the Rockwood School District wireless network
- Utilizing the network including the email system for soliciting, advertising, fundraising, commercial purposes or for financial gain, unless authorized by the district
- Utilizing the network for gambling or other illegal activities



INTERNET ACCESS AND USAGE

- Claiming copyright privileges over files, data and/or materials developed within the scope of employment
- Violating any copyright laws
- Downloading, distributing or copying copyrighted software in violation of copyright laws
- Downloading, distributing or copying copyrighted music, videos, or any type of data in violation with copyright laws
- Downloading or installing any software package without the approval of the Technology Department
- Downloading onto district computers legally obtained music or video files that are not required for school assignments or instructional purposes
- Using streaming media players (audio or video) that are not required for school assignments or instructional purposes
- Sending anonymous email.

The Rockwood School District will not be responsible or liable for any of the following:

- Information retrieved or lost through the district's computers or network
- Information stored by users on the district's diskettes, hard drives, file servers or other media
- Damage to personal property as a result of accessing the district's network and/or computers
- Controversial information and materials not blocked by the district's Internet filtering system
- User financial obligations caused by the authorized or unauthorized purchase of goods and/or services via the district's network.

Relevant Policies and Regulations

Policy 6321: <https://rsdmo.info/Policy6321>

Regulation 6321: <https://rsdmo.info/Regulation6321>

Agreement

I have read the above and understand my responsibility when using e-mail or Internet access and the consequences should I violate these guidelines.

Name (printed) _____ Date _____

Signature _____