

Red Oak Community School District

Technology Acceptable Use Policy

Introduction

Because 21st century skills are a vital part of the school district curriculum and management of district business, appropriate technologies will be made available to employees and students. These resources include access to the Internet and other network files or accounts by using computers or other digital devices that may or may not be owned by the district. Appropriate and equitable use of the Internet will allow employees and students to access resources unavailable through outdated means.

Students will be able to access the Internet through their teachers. Students, faculty, and staff may hold network accounts and district-issued email accounts. The person in whose name an account is issued is responsible at all times for its proper use. If a student already has an electronic mail address, the student may, with the permission of the supervising teacher, be permitted to use the address to send and receive mail at school. The district trusts assigned users to make responsible use of computing resources. The district also maintains a guest network that provides Internet access only. Users of the guest network are expected to comply with the current Technology Acceptable Use Policy. Employees and students will be instructed on the appropriate use of the Internet.

The Internet can provide a vast collection of educational resources for students and employees. It is a global network, which makes it impossible to control all available information. Because information appears, disappears and changes constantly, it is not possible to predict or control what students may locate. The school district makes no guarantees as to the accuracy of information received on the Internet. Although students will be under teacher supervision while on the network, it is not possible to constantly monitor individual students and what they are accessing on the network. Some students might encounter information that may not be of educational value. Student Internet records are confidential records treated like other student records. Students' Internet activities will be monitored by the school district to ensure students are not accessing inappropriate sites that have visual or textual depictions that include obscenity, child pornography or are harmful to minors. The school district will use technology protection measures to protect students from inappropriate access, including sites that include obscenity, child pornography or are harmful to minors.

The school district will monitor the online activities of students and will educate students about appropriate online behavior, including interacting on social networking sites and chat rooms. Students will also be educated on cyberbullying, including awareness and response. Employees will provide age appropriate training for students who use the Internet. The training provided will be designed to promote the school district's commitment to:

- The standards and acceptable use of Internet services as set forth in the Internet Safety Policy;
- Student safety with regard to:
 - safety on the Internet;
 - appropriate behavior while on online, on social networking Web sites, and
 - in chat rooms; and
 - cyberbullying awareness and response.
- Compliance with the E-rate requirements of the Children's Internet Protection Act

In this digital age, student records, assignments, and on-line classes are often available via the Internet. Red Oak Community School District will implement appropriate security measures to ensure that data is available only to those who have valid reason to access the data. It is the responsibility of parents, students, and district staff to keep passwords confidential and change passwords periodically.

Employee, Student, and Parent/Guardian Agreements

All employees, students and parents are expected to read the Red Oak Community School District Technology Acceptable Use Policy. All employees are required to sign the Red Oak Community School District Employee Technology Usage Agreement.

Parents/guardians of all students under the age of 18 are required to sign the Red Oak Community School District Student Access Release and Authorization Agreement before students will be granted access to the district's technology resources. This will be available upon registration. If for any reason, a parent or guardian does not want his/her student to have Internet access, then he/she must notify the district in writing. If access is removed at any time, the agreement must be resubmitted. Students in grades 6-12 will sign a form acknowledging they have read and understand the Internet Acceptable Use policy and regulations, that they will comply with the policy and regulations, and that they understand the consequences for violation of policy or regulations.

Students and parents of students who are provided a laptop through the One to One program must read the Student/Parent Laptop Handbook. A signed Laptop Computer Use Agreement must be on file with the District Technology Director prior to that student receiving a laptop computer.

Ownership

Access to computing resources is a privilege, not a right and the privilege can be suspended immediately without notice. All user accounts issued by the district are considered property of the district. The district allows users to access some or all of these resources for the reasons listed in this policy. These user guidelines extend beyond the school district's physical building, such as school issued email accounts, hardware, or software used when off the school district's property. Staff members or students will not retain proprietary rights related to the materials designed or created by such user if district hardware/software is used unless those rights are transferred to the user.

Network access, Internet access, and hardware are provided to support the educational goals set forth by the Board of Directors and to contribute to efficient management of district business. The district has the responsibility to maintain the integrity, operation, and availability of its hardware and network for access and use. The district does not guarantee user privacy or system reliability. It is not liable for loss or corruption of data resulting from using district-owned hardware or network resources.

Occasionally, through routine monitoring or maintenance, duly authorized personnel have authority to access individual files or data. Users should not expect that anything stored on school computers or networks will be private. Software may be used to monitor computer usage, system information, and remotely observe and manage network technology.

Electronic Communication

Electronic forms of communication have become the norm in many aspects of the educational process and management of a school. This includes, but is not limited to email, certain social media, discussion boards, and blogs. The Red Oak Community School District will grant email and other accounts to staff members and students as needed. These accounts are owned by the district and can be terminated at any time. Students will have their accounts disabled upon graduation or on their last day of enrollment at Red Oak Community Schools. Staff members leaving the district will have their accounts disabled as of their final contract day unless other arrangements are made.

In compliance with federal law, this policy will be maintained at least five years beyond the termination of funding under the Children's Internet Protection Act (CIPA) or E-rate.

INTERNET - APPROPRIATE USE REGULATION

I. Responsibility for Internet Appropriate Use.

- A. The authority for appropriate use of electronic Internet resources is delegated to the licensed employees.
- B. Instruction in the proper use of the Internet will be available to employees who will then provide similar instruction to their students.
- C. Employees are expected to practice appropriate use of the Internet, and violations may result in discipline up to, and including, discharge. Violations relating to or supporting of illegal activities will be reported to law enforcement agencies.

II. Internet Access.

- A. Access to the Internet is available to teachers and students as a source of information and a vehicle of communication.
- B. Students will be able to access the Internet while at school under the supervision of a staff member. Individual student accounts and electronic mail addresses may be issued to students at this time.
 - 1. Making Internet access available to students carries with it the potential that some students might encounter information that may not be appropriate for students. However, on a global network, it is impossible to control all materials. Because information on the Internet appears, disappears and changes, it is not possible to predict or control what students may locate.
 - 2. It is a goal to allow teachers and students access to the rich opportunities on the Internet, while we protect the rights of students and parents who choose not to risk exposure to questionable material.
 - 3. The smooth operation of the network relies upon the proper conduct of the end users who must adhere to strict guidelines which require efficient, ethical and legal utilization of network resources.
 - 4. To reduce unnecessary system traffic, users may use real-time conference features such as talk/chat/Internet relay chat only as approved by the supervising teacher.
 - 5. Transmission of material, information or software in violation of any board policy or regulation is prohibited.
 - 6. Users will be allowed to download and upload files that pass the requirements of the virus protection and/or content filter technologies that are in place.
 - 7. The school district makes no guarantees as to the accuracy of information received on the Internet.

III. Permission to Use Internet

- A. Annually, parents of students under the age of 18 will grant permission for their student to use the Internet using the prescribed form.
- B. All employees will sign the "District Employee Technology Usage Agreement" and return it to the Central Office.
- C. People using the guest wireless network to access the Internet will be required to agree to the terms of use before they are granted access.

IV. Student Use of Internet.

- A. Equal Opportunity - The Internet is available to all students who have permission to use the Internet within the school district under the supervision of a staff member. The amount of time available for each student may be limited by the number of available terminals and the demands for each terminal.
 - 1. It is possible that students in grades 6-12 who have a school-issued device as part of the 1:1 program will access the Internet without direct supervision of a staff member during the school day.
 - 2. Students in grades 6-12 who have a school-issued device as part of the 1:1 program will be able to access the Internet while away from school. Because they will be accessing the Internet via the school's Internet service and content filtering technology, the same rules apply.
 - 3. The Internet is available to all staff that has a District Employee Technology Usage Agreement on file with Central Office.
- B. Digital Citizenship
 - 1. The use of the network is a privilege and may be taken away for violation of board policy or regulations. As a user of the Internet, employees and students may be allowed access to other networks. Each network may have its own set of policies and procedures. It is the user's responsibility to abide by the policies and procedures of these other networks.

INTERNET - APPROPRIATE USE REGULATION

2. Internet Safety
 - a. Users shall not post personal contact information on the Internet with district-owned devices. This includes name, age, gender, home address, or telephone number. This does not include posts made on the school's learning management system.
 - b. Users should not share personal photos, personal videos, or photos/videos of others that do not support the curriculum or that are inappropriate.
 - c. Students shall not engage in instant messaging or social networking sites at any time during the school day except when such has been approved for classroom use.
 - d. Students should inform district personnel of any threatening, derogatory, or obscene communication immediately.
3. Cyberbullying— The Board Policy forbids cyberbullying. For the purposes of this policy, “cyberbullying” shall mean using digital communication capabilities on any electronic device to bully others by:
 - a. Sending or posting cruel messages or images
 - b. Threatening others
 - c. Excluding or attempting to exclude others from activities or organizations.
 - d. Starting or passing on rumors about others or the school system.
 - e. Harassing or intimidating others.
 - f. Sending angry, rude, or vulgar messages directed at a person or persons privately or to an online group.
 - g. Sending or posting harmful, untrue or cruel statements about a person to others.
 - h. Pretending to be someone else and sending or posting material that makes that person look bad or places that person in potential danger.
 - i. Sending or posting material about a person that contains sensitive, private, or embarrassing information, including forwarding private messages or images.
 - j. Engaging in tricks to solicit embarrassing information that is then made public.
4. Employees and students should adhere to on-line protocol:
 - a. Respect all copyright and license agreements.
 - b. Cite all quotes, references and sources.
 - c. Remain on the system long enough to get needed information, then exit the system.
 - d. Apply the same privacy, ethical and educational considerations utilized in other forms of communication.
 - e. **Copyright**—The Red Oak School District views copyright as a critical issue in regards to 21st Century learning. Copyright, and the related areas of trademark and licensing, are one of the most important issues to be addressed and taught to students. Copyright protects the rights of creators and users of information. Students and staff members of the Red Oak Community School District are expected to follow copyright law.
 - 1) **Plagiarism**—The dictionary defines plagiarism as “taking ideas or writings from another person and offering them as your own.” The person who leads readers to believe that they are reading original work when it is copied, is guilty of plagiarism. The person who created a piece of work, should always be given credit. With the amount of cutting and pasting that is done via the Internet, it is important that the guidelines of plagiarism are followed and credit is always given to the author of any piece of work.
 - 2) **Fair Use**—Fair use is part of the copyright law, and can be used when completing school work. If copying is not specifically prohibited in the copyright law, then it may be allowed under fair use. Users need to make good decisions about the specific circumstances in which they are using others' work. Students and employees of the Red Oak School District are expected to follow the fair use guidelines that are provided in the Board Policy Manual.
 - 3) **Public Domain**—Users may upload creative works that are in the public domain for their own use. Users are responsible for determining whether a program is in the public domain.
 - 4) **File Sharing**—The installation and/or use of any Internet-based file-sharing tools is prohibited. File-sharing programs and protocols like BitTorrent, Limewire, Kazaa, Acquisition and others may not be used to facilitate the illegal sharing of copyrighted material (music, video, and images).
5. Email—Employees and Students should use only district-assigned email accounts or other approved forms of digital communication while at school. Employees and students are expected to adhere to the following guidelines:
 - a. School-issued email accounts will be accessed using the district supported and approved client software.
 - b. Users are responsible for their passwords and accounts. At no time should one share his or her passwords with other users. Users are not to use, or allow others to use their email or other accounts. Any inappropriate use can result in the loss of the account as specified in the Acceptable Use Policy.

INTERNET - APPROPRIATE USE REGULATION

- c. Information transported using district email and other district owned accounts is not to be considered private, secure, or confidential. All electronic communication generated on district-owned hardware is considered the property of the school district and may be reviewed and deleted as needed to ensure network integrity and confidentiality.
 - d. Email and other electronic communication should reflect professional standards at all time. School accounts should only be used for school related correspondence. With regards to personal email use, occasional sending or receiving of personal messages by staff or students is inevitable. This type of incidental personal use is permitted providing it does not violate district policy, adversely affect others, the speed of the network, or the employee's professional responsibilities, including using instructional time for personal communication.
 - e. District owned resources should never be used for the conduct of any personal, discriminatory, or unlawful business. This includes use for commercial purposes, advertising, and political lobbying.
 - f. In addition to the regulations listed above, users are expected to adhere to the following guidelines:
 - 1) Read email on a regular basis
 - 2) Delete unwanted messages immediately
 - 3) Use of vulgar and/or abusive language is prohibited
 - 4) Always sign your name to a message
 - 5) Acknowledge that you have received a document or file that someone has sent to you
- C. Restricted Material
1. Employees and students will not intentionally access, transmit, or download any text file or or engage in any conference that:
 - a. includes material which is obscene, libelous, indecent, vulgar, profane or lewd.
 - b. advertises any product or service not permitted to minors by law.
 - c. constitutes insulting or fighting words, the very expression of which injures or harasses others.
 - d. presents a clear and present likelihood that, either because of its content or the manner of distribution, it will cause a material and substantial disruption of the proper and orderly operation and discipline of the school or school activities.
 - e. will cause the commission of unlawful acts or the violation of lawful school regulations.
 2. Users agree to inform an appropriate district employee immediately if he or she:
 - a. accidentally enters an internet site that is inappropriate as defined by this policy.
 - b. accidentally changes the configurations on any computer.
 - c. receives a message which makes him or her uncomfortable or is offensive.
 3. Use of social network sites, game sites, chat rooms, and other similar sites, except under the direction of a classroom teacher during instructional hours is prohibited.
 4. Any user of district technology resources used in the context of the school is prohibited from viewing, sending, or composing any digital communication that indicates or suggests unethical or illegal solicitation, racism, sexism, language that is inappropriate for the educational setting, cyberbullying, harassment, pornography, and other issues, including those defined by the nondiscrimination policy of the district.
 5. Employees and students are prohibited from installing any unauthorized software, including personally owned software, on district-owned computers without permission from the district technology director.
 6. All users are responsible for ensuring that any storage media that is brought in from outside the school are virus free and do not contain any unauthorized or inappropriate files as defined in this document.
- D. Unauthorized Costs - If an employee or student gains access to any service via the Internet which has a cost involved or if an employee or student incurs other types of costs, the user accessing such a service will be responsible for those costs.
- E. Abuse of Network Privileges
1. Employees and students will not use the network in such a way that would disrupt the use of the network by others.
 - a. Users should never share their password with anyone or use another user's password.
 - 1) Users who share their passwords will be considered responsible any results of such use.
 - 2) If a user believes others know their password and if any user files have been altered, he or she should notify a district employee.
 - b. Students should never use teachers' computers without permission or supervision.
 - c. Teachers should never allow students to use any device while the teacher is logged in.
 - d. Gaining or attempting to gain unauthorized access to others' files or vandalizing the data of another user is prohibited.

INTERNET - APPROPRIATE USE REGULATION

- F. Vandalism is not permitted and will be strictly disciplined.
 - 1. Vandalism is defined as any attempt to harm or destroy computer equipment as well as the data of another user or of another agency or network that is connected to the Internet.
 - 2. Vandalism includes, but is not limited to the uploading, downloading, or creation of computer viruses, or programs that infiltrate computer systems and/or damage software components.

- V. District Rights and Responsibilities
 - A. Teachers and those assisting students are responsible for teaching proper techniques and standards for participation, for guiding student access to appropriate areas of the Internet, for assuring that students understand what constitutes misuse of the Internet, and the consequences of misuse. Teachers should model appropriate behavior and enforce the Acceptable Use Agreement.
 - B. The district shall provide all reasonable software for use by staff and students.
 - C. All software/hardware purchases need approval of the District Technology Coordinator.
 - D. Red Oak Community School District reserves the right to monitor all activity and use of the network. This includes, but is not limited to, monitoring downloads, files, and documents stored on any school-owned hardware, checking Internet histories and cache files, observing users' screens, reading email if deemed necessary, and blocking what the district considers inappropriate sites.
 - E. The district technology staff routinely monitors and performs maintenance on file servers, email, workstations, the Internet, and user accounts. During these procedures, it may be necessary to review email and/or files stored on the network. Users should avoid storing personal and/or private information on the district and/or school's technology resources.
 - F. If routine maintenance and monitoring of the district's systems shows that a user has violated this agreement, another school district agreement or law, school district officials will conduct an individual investigation or search.
 - G. Sanctions may be both internal, involving loss of privileges or other district measures; and external, involving civil or criminal action under state or federal laws. All inappropriate items can be confiscated and only be returned to a parent/guardian.

- VI. Student Violations--Consequences and Notifications.
 - A. Students who access restricted items on the Internet are subject to the appropriate action described in board policy or regulations or the consequences found in the table on the next page.
 - B. Parents/Guardians will be notified of all violations of this Acceptable Use Agreement in a written letter or email from a school administrator or the technology coordinator.