APPENDIX A:

Internet Safety Policy & Acceptable Use of Technology Resources

Red Oak Independent School District

Internet Safety Policy

Introduction

It is the policy of the Red Oak Independent School District ("ROISD") 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 ("CIPA"). It is the goal of this policy not only to prevent and protect, but to educate employees, students, parents and the community of ROISD in Internet safety. The CIPA guidelines for an Internet Safety Policy have also been incorporated by ROISD into its Technology Resource Acceptable Use Policy.

The Children's Internet Protection Act, enacted December 21, 2000, requires recipients of federal technology funds to comply with certain Internet filtering and policy requirements. Schools and libraries receiving funds for Internet access and/or internal connection services must also meet the Internet safety policies of the Neighborhood Children's Internet Protection Act ("NCIPA") that addresses the broader issues of electronic messaging, disclosure of personal information of minors, and unlawful online activities. In addition, Texas House Bill No. 18, the Securing Children Online through Parental Empowerment (SCOPE) Act, enacted June 13, 2023, requires covered digital service providers to provide minors with certain data protections, prevent minors from accessing harmful content, and give parents tools to manage their child's use of the service.

This policy is intended to be read together with the ROISD's Technology Resource Acceptable Use Policy. All limitations and penalties set forth in the Technology Resource Acceptable Use Policy are deemed to be incorporated into this policy. Terms used in this policy which also appear in the Children's Internet Protection Act have the meanings defined in the Children's Internet Protection Act.

COMPLIANCE WITH THE REQUIREMENTS OF CIPA:

Technology Protection Measures

A Technology Protection Measure is a specific technology that blocks or filters Internet access. It must protect against access by adults and minors to visual depictions that are obscene, involve child pornography, or are harmful to minors. ROISD utilizes a sophisticated content filtering system located at the firewall level to ensure all computers are subject to filtering that is compliant with CIPA and NCIPA.

Access to Inappropriate Material

To the extent practical, Technology Protection Measures (or "Internet filters") shall be used to block or filter the Internet, or other forms of electronic communications, access to inappropriate information. Specifically, as required by CIPA and SCOPE, blocking shall be applied to visual and textual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. Subject to administrative approval, Technology Protection Measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes. Any attempt to bypass, defeat or circumvent the Technology Protection Measures is punishable as a violation of this policy and of the Technology Resource Acceptable Use Policy.

Inappropriate Network Usage

To the extent practical, steps shall be taken to promote the safety and security of users of the ROISD online computer network when using electronic mail, chat rooms, blogging, instant messaging, online discussions and other forms of direct electronic communications. Without limiting the foregoing, access to such means of communication is strictly limited by the Technology Resource Acceptable Use Policy. Specifically, as required by CIPA and SCOPE 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 professional employees (pedagogical and administrative staff) of ROISD to supervise and monitor usage of the school district's computers, computer network and access to the Internet in accordance with this policy, the Technology Resource Acceptable Use Policy, and CIPA and SCOPE Act. In accordance with SCOPE Act, ROISD has secured an internet filtering software that blocks inappropriate content and alerts administrators if students attempt to access such content. Campus administration will notify parents regarding alerts of inappropriate use. Procedures for the disabling or otherwise modifying any Technology Protection Measures shall be the responsibility of the Director of Technology or designated representatives.

Education

ROISD will advocate and educate employees, students, parents and the ROISD community on Internet safety and "cyber-bullying." In accordance with the SCOPE Act, parent education will be provided through such means as professional development training and materials to employees, PTA presentations, Parent University and the school district website.

Cyber-bullying

The Technology Resource Acceptable Use Policy includes provisions intended to prohibit and establish penalties for inappropriate and oppressive conduct, including cyber-bullying. ROISD is a place of tolerance and good manners.

- Students may not use the network or any ROISD computer facilities for hate mail, defamatory statements, statements intended to injure or humiliate others by disclosure of personal information (whether true or false), personal attacks on others, and statements expressing animus towards any person or group by reason of race, color, religion, national origin, gender, sexual orientation or disability.
- Network users may not use vulgar, derogatory, or obscene language.
- Network users may not post inappropriate anonymous messages or forge e-mail or other messages.
- ROISD computers and network facilities may not be used for any activity, or to transmit any material, that violates United States, State of Texas or local laws. This includes, but is not limited to, any threat or act of intimidation or harassment against another person.

Time Restrictions

In accordance with the SCOPE Act, Red Oak ISD has implemented time restrictions on student devices. All elementary student devices will remain on campus. Within the instructional day, teachers will use a combination of digital and non-digital instructional strategies. In addition, in the event of a cybersecurity situation, ROISD may be required to disable student devices to mitigate the threat until a solution has been determined.

Data Privacy

Red Oak ISD will adopt software applications that collect only the data strictly necessary for educational purposes. Online resources and applications will be approved through a semi-annual district process. A list of approved applications is available on the ROISD Instructional Technology website.

Red Oak Independent School District

Technology Resource Acceptable Use Policy

Introduction

Red Oak Independent School District makes a variety of communication and information technologies available to students, employees, and other authorized users to enhance the learning environment and promote educational excellence. These technologies, when properly used, will provide educational benefits to students and employees through resource sharing, innovation and communication. The purpose of this Acceptable Use Policy is to educate district students, employees, and authorized users of the rules and standards of behavior to be followed when using the district technology resources, as well as the consequences for failing to meet those rules and standards. The district firmly believes that the valuable information and interaction available through the use of the district technology resources far outweighs the possibility that users may interact with material that is not consistent with the district's educational goals.

Mandatory Review

To educate district employees, students, and authorized users on proper Technology Resource use and conduct, all users are required to review these guidelines at the beginning of each school year. All district employees shall be required to acknowledge receipt and understanding of all administrative regulations governing use of the system and shall agree in writing to allow monitoring of their use and to comply with such regulations and guidelines. Both the student and parent or legal guardian are required to acknowledge receipt and understanding of the Acceptable Use Policy as part of their review of the Discipline Management Plan and Student Code of Conduct handbook. All such receipts will be maintained on file in the principal's or departmental supervisor's office. Employees supervising students who use the district's system must provide training emphasizing its appropriate use.

District Technology Resources

District Technology Resources refers to any configuration of hardware and software operated and provided by Red Oak ISD, including electronic computer systems, data management systems, and communication infrastructure. The system includes but is not limited to the following:

- Telephones, cellular telephones, pagers and voicemail facilities;
- Data communications network, Wi-Fi;
- Electronic mail (e-mail) accounts;
- Printers, copiers, fax machines;
- Servers;
- Computer hardware and peripherals;
- Software including operating system software and application software;
- Digitized information including stored text, data files, e-mail, digital images and audio files;
- Internally accessed databases or tools;
- Externally accessed databases (such as the Internet); and,
- Additional technologies as they become available.

Acceptable Use

Technology Resources will be used to improve learning and teaching consistent with the district's educational goals. The district requires legal, ethical and appropriate use of all Technology Resources.

Access to Technology Resources. Network and Internet access is provided to all district teachers and staff. Students may be allowed to use the local network with campus permission, but may only use the Internet with parent permission. All Internet access will be monitored by district staff. All non-employee/non-student users must obtain approval from the Technology Director or designee to gain individual access to the district's system.

Access to the district's electronic communications system, including the Internet, shall be made available to students and employees primarily for instructional and administrative purposes and in accordance with administrative regulations. Limited personal use is permitted if the use imposes no tangible cost to the district, does not unduly burden the district's computer or network resources, and has no adverse effect on an employee's job performance or on a student's academic performance.

Privilege. Access to the district's technology resources is a privilege, not a right. As such access may be denied for any individual for any reason at the district's sole discretion.

Content/Third-Party Supplied Information. System users and parents of students with access to the district's system should be aware that use of the system may provide access to other electronic communications systems in the global electronic network that may contain inaccurate and/or objectionable material. A user who gains access to such material is expected to discontinue the access as quickly as possible and to report the incident to the supervising staff member.

Security

System security is a high priority and the responsibility of all system users.

Reporting Security Problem. If knowledge of inappropriate material or a security problem on the district technology resources is identified, the user should immediately notify the district's Help Desk or supervising staff member. The security problem should not be shared with others.

Accounts. Staff, students, and other authorized users who are assigned individual accounts will be held responsible for any and all activity logged under that account. When any user under a district issued account violates district policy, the district shall attribute this conduct to the individual assigned the account. Allowing a third party to use a district provided account shall not be a defense to student or employee discipline. System users may not use another person's system account.

Passwords. Passwords are the primary way in which users are authenticated and allowed to use the district's computing resources. System users are required to maintain password confidentiality by not sharing their password with others recognizing that if they do so, they will be held accountable for their actions as well as those of other parties to whom they have given access.

Filtering. Sites accessible via district technology resources may contain material that is illegal, defamatory, inaccurate or controversial. Each district computer with Internet access has filtering software that blocks access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children's Internet Protection Act and SCOPE Act. The district makes every effort to limit access to objectionable material; however, controlling all of such materials on the Internet is impossible, even with filtering in place. With global access to computers and people, a risk exists that students may access material that may be inappropriate and not of educational value in the school setting. The Red Oak Internet connection is the only system to be used in schools. No commercial Internet accounts may be used.

Data Privacy. In order to provide students with access to online applications and resources, the district will share only the data strictly necessary for educational purposes. The district will semi-annually review data privacy agreements and ensure measures are taken to safely and securely share required information. Student personal identifiable information is only shared with district approved resources. Parents are encouraged to review the list of approved resources on the district's Instructional Technology website. Additionally, unapproved software applications conducting non-educational assessments or collecting information about students is strictly prohibited.

Monitoring

All district system usage is subject to monitoring by designated staff at any time to ensure appropriate use. Users should treat the computer system like a shared or common file system with the expectation that electronic files, sent, received or stored anywhere in the computer system will be available for review by any authorized representative of the district, and may be subject to public disclosure under the Texas Public Information Act. System users should not use the computer system to send, receive or store any information, including e-mail messages, that they consider personal or confidential and wish to keep private. The district reserves the right to access, review, modify, copy, delete, or disclose such information for any purpose. District staff will monitor and examine all users of the district's systems to ensure appropriate and ethical use.

Inappropriate Use

Inappropriate use includes, but is not limited to, those uses that violate the law, that are specifically named as violations in this document, that violate the rules of network etiquette, or that hamper the integrity or security of this or any components that are connected to the Computer/Network/Internet. The following actions are considered inappropriate uses and are prohibited:

Transmission of any material in violation of any federal or state law is prohibited. This includes, but is not limited to:

- copyrighted material;
- plagiarized material;
- threatening, harassing, defamatory or obscene material;
- material protected by trade secret.

Bullying. Any use of district technology resources to threaten, harass, defame, humiliate, embarrass, or otherwise target another person is prohibited.

Intellectual Property. Teachers, staff, and students must always respect copyrights and trademarks of third-parties and their ownership claims in images, text, video and audio material, software, information, and inventions. The copy, use, or transfer of others' materials without appropriate authorization is not allowed.

Impersonation/Plagiarism. Fraudulently altering or copying documents or files authored by another individual is prohibited. Fraudulently creating a document or communication and attributing it to another is prohibited. Assuming the identity of another individual is prohibited.

File/Data Violations. Deleting, examining, copying, or modifying files and/or data belonging to other users, without their permission or district authorization is prohibited.

Hacking/Circumvention. Any attempt to hack or circumvent district firewalls, filters, or system security is prohibited. Unauthorized access of district systems and data strictly is prohibited.

Transmitting Confidential Information. Teachers, staff, and students may not redistribute or forward confidential information (i.e. educational records, directory information, personnel records, etc.) without proper authorization. Confidential information should never be transmitted, redistributed or forwarded to outside individuals who are not expressly authorized to receive the information. Revealing such personal information as home addresses or phone numbers of users or others is prohibited.

Modification of Computer. Modifying or changing computer settings and/or internal or external configurations without appropriate permission is prohibited. Adding or removing any software or hardware without written permission from the Technology Director or designee is prohibited. Tampering with or theft of components from district systems may be regarded as criminal activity under applicable state and federal laws.

Commercial Use. Use of the system for any type of income-generating activity is prohibited. Advertising the sale of products, whether commercial or personal is prohibited.

Marketing by Non-ROISD Organizations. Use of the system for promoting activities or events for individuals or organizations not directly affiliated with or approved by the district is prohibited.

Political Lobbying. Consistent with State ethics laws, district resources and equipment, including, but not limited to, e-mail, must not be used to conduct any political activities, including political advertising or lobbying.

Vandalism/Mischief. Any malicious attempt to harm or destroy district equipment, materials or data; or the malicious attempt to harm or destroy data of another user of the district's system, or any of the agencies or other networks to which the district has access is prohibited. Any deliberate attempt to degrade or disrupt system performance is prohibited.

Consequences of Inappropriate Use

Violations of Red Oak ISD's policies and procedures concerning the appropriate use of district technology resources may result in the suspension of access, termination of privileges, and/or other disciplinary action consistent with board policies, the Student Code of Conduct, and State or Federal law. This may also require restitution for costs associates with system restoration, hardware, or software costs. The district will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the district's technology resources.

Electronic Communication

Electronic communication encompasses all communication sent via technological devices. It may include email, websites, electronic documents, electronic images, electronic sound, electronic video, and social media such as blogs, wikis, forums, and messages boards. All staff, students, parents, and authorized users should be aware of their responsibility to use these resources in a positive manner. The district encourages the use of electronic communication to enhance the learning environment consistent with the district's educational goals.

Social Media. Students and employees may participate in social media learning environments (such as, but not limited to, blogs, discussion forums, RSS feeds, wikis, and message boards) within a district-approved safe, secure, curriculum-supported learning opportunity.

Electronic Mail. Electronic Mail (e-mail) is one of the most used communications tools in the district. All teachers and staff are issued e-mail accounts for instructional and administrative needs. Users should check e-mail frequently, delete unwanted messages promptly. E-mail attachments are limited to 15MB or smaller.

Perceived Representation. Users should be aware, school-related electronic communications may cause some recipients or other readers to assume that the user's comments represent the district or school, whether or not that was the user's intention.

Privacy. Electronic communication should not be considered private. Users should be aware that any electronic communication may become public information, available for view by any person or entity. Confidential information, such as home addresses or phone numbers, should not be divulged in electronic communications without the permission of the individual involved.

Inappropriate Language. Using obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language in electronic communications distributed through district technology resources is prohibited. Sending messages that could cause danger or disruption, personal attacks, including prejudicial or discriminatory attacks are prohibited.

Forgery. Forgery or attempted forgery of e-mail messages or other electronic communications is prohibited and punishable by law. Attempts to read, delete, copy, or modify the communications of other system users, deliberate interference with the ability of other system users to utilize electronic communication, or the use of another person's user ID and/or password is prohibited.

Junk Mail/Chain Letters. Generally users should refrain from forwarding e-mails or communications which do not relate to the educational purposes of the district. Chain letters or other e-mails intended for forwarding or distributing to others is prohibited. Creating or distributing unnecessary messages to people (spamming) is also prohibited.

Resource Usage. Users should limit electronic communications to instructional and administrative functions.

Student E-mail Accounts. Student e-mail accounts may be provided directly by the district or through the content management system of an approved online course. As appropriate and with written approval of the designated district personnel in the Technology Department, project e-mail accounts will be granted for specific educational activities. Students who are given access to an e-mail account are expected to abide by the guidelines established for Electronic Communication.

Students are prohibited from accessing personal electronic communication accounts (e-mail, Facebook, Twitter, etc.) using the district's system.

Display of Student Information on District Websites. The following conditions apply to the display of student information on district websites. A content contributor who knowingly violates (or promotes the violation of) any portion of these guidelines will be subject to disciplinary action in accordance with district policies.

Student-created projects, Writings, and/or artwork are permitted on campus/district websites if the appropriate parental/student consent has been obtained.

Student photographs or names are permitted if the directory information specified for the student allows for it.

All student photographs and/or student work may be displayed without the student's name. No other personal student information is allowed including, but not limited to, name, e-mail address, phone number, home address, and/or birth date.

Disclaimer

The district's system is provided on an "as is, as available" basis. The district does not make any warranties, whether express or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The district does not warrant that the functions or services performed by, or that the information or software contained on the system will meet the system user's requirements, or that the system will be uninterrupted or error free, or that defects will be corrected.

Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third-party individuals in the system are those of the providers and not the district. The district will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the district's electronic communications system.

Elastic Clause. The school and administration reserve the right to establish fair and reasonable rules and regulations for circumstances that may arise requiring actions that are not covered under these guidelines. In all cases, rules, regulations, and possible consequences shall be as consistent as possible with previously established rules, regulations, and consequences for similar incidents.

Matters omitted from these guidelines should not be interpreted as a limitation to the scope of the district's responsibility and, therefore, the district's authority in dealing with any type of infraction that may not be in the best interest of the safety and welfare of the students.

These rules and policies apply to any student who is on school property, who is in attendance at school or any school-sponsored activity, or whose conduct at any time or place directly interferes with the operations, discipline, or general welfare of the district, schools, students and staff.

More Information

These guidelines were developed pursuant to Board Policy CQ(LOCAL). More information can be found at the following locations:

- **Red Oak ISD Board Policies**
- **Student Code of Conduct**
- **Employee Handbook**