

East Otero School District R-1- La Junta Public Schools Student/Staff Information Technology Resources Acceptable Use Rules and Procedures

East Otero School District R-1 is providing students/staff access to the district's electronic network. This network includes Internet access, computer services, computer equipment and related equipment for educational purposes. The purpose of this network is to assist in preparing students/staff for success in life and work in the 21st century by providing them with electronic access to a wide range of information and the ability to communicate with people throughout the world. This document contains the rules and procedures for students'/staff acceptable use of the East Otero School District R-1 electronic network.

The East Otero School District R-1 Internet system is filtered as required by the Children's Internet Protection Act, but no filtering system is capable of blocking 100% of the inappropriate material available on the Internet. Parents should be warned that some material accessible via the Internet might contain items that are illegal, defamatory, inaccurate or potentially offensive to some people. While our intent is to make Internet access available to further educational goals and objectives, students may find ways to access other materials as well. Students or staff who abuse acceptable use, which includes, but is not limited to: copyrighted material, threatening or obscene material, pornography, gambling, and inappropriate language will be subject to discipline.

- The East Otero School District R-1 electronic network has been established for a limited educational purpose. The term "educational purpose" includes classroom activities, career development, and limited high-quality self-discovery activities.
- The East Otero School District R-1 electronic network has not been established as a public access service or a public forum. East Otero School District R-1 has the right to place reasonable restrictions on material that is accessed or posted throughout the network.
- Parent/guardian permission is required for all students under the age of 18. Access is a privilege — not a right.
- It is presumed that students/staff will honor this agreement they and their parent/guardian have signed. The district is not responsible for the actions of students/staff who violate them beyond the clarification of standards outlined in this policy.
- The district reserves the right to monitor all activity on this electronic network. Students/Staff will indemnify the district for any damage that is caused by students'/staff inappropriate use of the network.
- Students/Staff are expected to follow the same rules, good manners and common sense guidelines that are used with other daily school activities in the use of the East Otero School District R-1 electronic network.

General Unacceptable Behavior

While utilizing any portion of the East Otero School District R-1 electronic network, unacceptable behaviors include, but are not limited to, the following:

- Students/Staff will not post information that, if acted upon, could cause damage or danger of disruption.
- Students/Staff will not engage in personal attacks, including prejudicial or discriminatory attacks.
- Students/Staff will not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a student/staff is told by a person to stop sending messages, they must stop.
- Students/Staff will not knowingly or recklessly post false or defamatory information about a person or organization.
- Students/Staff will not attempt to access blocked Internet sites.

- Students/Staff will not use criminal speech or speech in the course of committing a crime such as threats to the president, instructions on breaking into computer networks, child pornography, drug dealing, purchase of alcohol, gang activities, threats to an individual, etc.
- Students/Staff will not use speech that is inappropriate in an educational setting or violates district rules.
- Students/Staff will not abuse network resources such as sending chain letters or "spamming".
- Students/Staff will not display, access or send offensive messages or pictures.
- Students/Staff will not use the East Otero School District R-1 electronic network for commercial purposes. Students/Staff will not offer, provide, or purchase products or services through this network.
- Students/Staff will not use the East Otero School District R-1 electronic network for political lobbying. Students/Staff may use the system to communicate with elected representatives and to express their opinions on political issues in a reasonable manner.
- Students/Staff will not attempt to access non-instructional district systems, such as student information systems or business systems other than is required for their job.
- Students/Staff will not use any wired or wireless network (including third party internet service providers) with equipment brought from home without permission from the technology department. Example: The use of a home computer on the network or accessing the internet from any device not owned by the district.
- Students/Staff will not use district equipment, network, or credentials to threaten employees, or cause a disruption to the educational program.
- Students/Staff will not use the district equipment, network, or credentials to send or post electronic messages that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.

E-Mail

- E-mail for students in the elementary grades will only be provided through a teacher or classroom e-mail account.
- Junior and Senior High School students may be provided with e-mail accounts with the approval of the building level administrator for specific educational projects or activities.
- Students will not establish or access Web-based e-mail accounts on commercial services through the district network unless such accounts have been approved for use by the individual school.
- Students/Staff will not repost a message that was sent to them privately without the permission of the person who sent them the message.
- Students/Staff will not post private information about another person.

World Wide Web

- Elementary School Level - Access to information for students on the Web will generally be limited to prescreened sites that are closely supervised by the teacher.
- Junior and High School Level - Access to information for students on the Web will generally be provided through prescreened sites and in a manner prescribed by their school.

Message Board/Usenet Groups

- The district may provide access to selected newsgroups that relate to subjects appropriate for educational use. Messages posted locally that are in violation of this policy will be removed. The district reserves the right to immediately terminate an account of a student or staff member who misuses the message boards or Usenet groups.

Real-time, Interactive Communication Areas (Note: Chat rooms are normally blocked)

- Students/Staff may use chat or instant messaging, but only under the direct supervision of a teacher or in a moderated environment that has been established to support educational activities and has been approved by the district or individual school and the technology department.

Web Sites

- Elementary and Junior High School Level - Group pictures without identification of individual students are permitted. Student work may be posted with either student first name only or other school-developed identifier (such as an alias or number).
- High School Level - Students may be identified by their full name with parental approval. Group or individual pictures of students with student identification are permitted with parental approval. Parents may elect to have their child assigned to the elementary/middle school level of use.
- Material placed on student Web pages are expected to meet academic standards of proper spelling, grammar and accuracy of information.
- Material (graphics, text, sound, etc.) that is the ownership of someone other than the student may not be used on Web sites unless formal permission has been obtained.
- All student Web pages should have a link back to the home page of the classroom, school or district, as appropriate.

Personal Safety

- Students will not share personal contact information about themselves or other people. Personal contact information includes address, telephone, school address, or work address.
- Elementary and Junior High School students will not disclose their full name or any other personal contact information for any purpose.
- High school students will not disclose personal contact information, except to education institutes for educational purposes, companies or other entities for career development purposes, or only with specific building administrative approval.
- Students will not agree to meet with someone they have met online.
- Students will promptly disclose to a teacher or other school employee any message received that is inappropriate or makes the student feel uncomfortable

System Security

- Students/Staff are responsible for their individual accounts and should take all reasonable precautions to prevent others from being able to use them. Under no condition should students/staff provide their password to another person other than technology department staff.
- Users will not attempt to access Web sites blocked by district policy, including the use of proxy services, software, or Web sites.
- Students/Staff must immediately notify a teacher or the system administrator if they have identified a possible security problem. Students/Staff should not go looking for security problems, because this may be construed as an illegal attempt to gain access.
- Students/Staff will not attempt to gain unauthorized access to any portion of the East Otero School District R-1 electronic network. This includes attempting to log in through another person's account or access another person's folders, work, or files. These actions may be construed as an illegal act, even if only for the purposes of "browsing".
- Students/Staff will not make deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or by any other means. These actions may be construed as an illegal act.
- Users will not use sniffing or remote access technology to monitor the network or other user's activity.

Software and Files

- Software is available to students/staff to be used as an educational resource. No student/staff may install, upload or download software without permission from the district technology department. Unauthorized software may be removed without notice.
- A student's account may be limited or terminated if a student intentionally misuses software on any district-owned equipment.

- Files stored on the network are treated in the same manner as other school storage areas, such as lockers. Routine maintenance and monitoring of the East Otero School District R-1 electronic network may lead to discovery that a student/staff member has violated this policy or the law. Students/Staff should not expect that files stored on district computers and/or servers are private or that they have any expectation of privacy.

Technology Hardware

- Hardware and peripherals are provided as tools for student use for educational purposes. Students/Staff are not permitted to relocate hardware, install peripherals or modify settings to equipment without the consent of the district technology department. Unauthorized equipment may be removed without notice.

Vandalism

- Any malicious attempt to harm or destroy data, the network, other network components connected to the network backbone, hardware or software will result in cancellation of network privileges. Disciplinary measures in compliance with the district's discipline code and policies will also be enforced.

Plagiarism and Copyright Infringement

- Students/Staff will not plagiarize works found on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were the students'.
- District policies on copyright will govern the use of material accessed and used through the district system.
- Copyrighted material will not be placed on any system without the author's permission. Permission may be specified in the document, on the system or must be obtained directly from the author.

Videoconference

- Videoconferencing is a way that students can communicate with other students, speakers, museums, etc. from other parts of the country and the world. With videoconferencing equipment, students/staff can see, hear, and speak with other students, speakers, museum personnel, etc. in real-time.
- Videoconference sessions may be videotaped by district personnel or by a participating school involved in the exchange in order to share the experience within ours or their building or district.
- Students/Staff voices, physical presence, and participation in the videoconference are transmitted to participating sites during each session. Rules and procedures relative to acceptable use and behavior by students/staff apply during all videoconference sessions.

Student/Staff Rights

- Students'/staffs' right to free speech applies to communication on the Internet. The East Otero School District R-1 electronic network is considered a limited forum, similar to the school newspaper, and therefore the district may restrict a student's/staffs' speech for valid educational reasons or as is otherwise allowed by law.
- An individual search will be conducted if there is reasonable suspicion that a student/staff has violated this policy or the law. The investigation will be reasonable and related to the suspected violation.

Due Process

- The district will cooperate as required by law with local, state, or federal officials in any investigation related to any illegal activities conducted through the district network.
- In the event there is an allegation that a student/staff has violated the district acceptable use rules and procedures, the student/staff member will be provided with a written notice of the alleged

violation. An opportunity will be provided to present an explanation before a neutral administrator (or student/staff member will be provided with notice and an opportunity to be heard in the manner set forth in the disciplinary code).

- Disciplinary actions will be tailored to meet specific concerns related to the violation and to assist the student/staff member in gaining the self-discipline necessary to behave appropriately on an electronic network. Violations of the acceptable use regulation and policy may result in a loss of access as well as other disciplinary or legal action.
- If the violation also involves a violation of other provisions of other school rules, it will be handled in a manner described in the school rules. Additional restrictions may be placed on a student's /staff members use of his/her network account.

Limitation of Liability

- The district makes no guarantee that the functions or the services provided by or through the district network will be error-free or without defect. The district will not be responsible for any actual or consequential damages suffered, including but not limited to, loss of data or interruptions of service.
- The district is not responsible for the accuracy or quality of the information obtained through or stored on the network. The district will not be responsible for financial obligations arising through the unauthorized use of the network.

Consequences for Violations of these Acceptable Use Rules and Procedures

Violations of these rules and procedures may result in loss of access as well as other disciplinary or legal action. Students' violation of these rules and procedures shall be subject to the consequences as indicated within this document as well as other appropriate discipline, which includes but is not limited to:

- Out of School Suspension (Mandatory 1-5 days, dependent on severity of abuse)
AND any of the following:
 - Use of district network only under direct supervision
 - Suspension of network privileges
 - Revocation of network privileges
 - Suspension of computer privileges
 - Expulsion from school and/or
 - Legal action and prosecution by the authorities

Staff violation of these rules and procedures shall be subject to appropriate discipline as set forth in district policy. The particular consequences for violations of these rules and procedures shall be determined by the school administrators. The superintendent or designee and/or the board shall determine when school expulsion and/or legal action or actions by the authorities are the appropriate course of action.

**East Otero School District R-1 - La Junta Public Schools
Student/Staff Information Technology Resources
User Agreement and Parent Permission**

To use the electronic information technology resources provided by the district, all students and staff must sign and return this form, and those under 18 years of age must obtain parental permission. I understand that the following is a non-exhaustive list of activities that will not be tolerated, and that violations may result in the loss of account privileges, as well as other disciplinary and/or legal action:

- Sending or displaying offensive messages or pictures
- Using obscene language
- Giving personal information, such as complete name, phone number, address, or identifiable photo, without permission from a teacher and parent or guardian
- Harassing, insulting or attacking others
- Damaging or modifying computers, computer systems or computer networks
- Violating copyright laws
- Using other's logins and/or passwords
- Trespassing in other's folders, work or files
- Intentionally wasting limited resources
- Attempting to circumvent network security.
- Employing the network for commercial purposes, financial gain, political lobbying, or fraud

Student/Staff User Agreement:

As a user of the La Junta Public Schools – East Otero R-1 School District electronic information technology resources, I hereby agree to comply with the statements and expectations outlined in this document and in the Acceptable Use Rules and Procedures, which I acknowledge receiving and reading, and to honor all relevant laws and restrictions. I also agree that East Otero School District R-1 reserves the right to access any information saved on District owned devices up to and including: Documents, Photos, Videos, Website Accounts that remained logged in (Facebook, Twitter, Instagram, etc.), or District maintained email accounts.

Student's/Staff's Full Name (Please Print): _____

Grade Level (K-8) or for HS Students Expected Year of Graduation _____

Parent's Name (if student is under age 18) _____

Street Address _____ City _____

Home Phone _____

Student's/Staff's Signature _____ Date _____

Parent/Guardian Permission:

All students are provided with access to district electronic information technology resources. In addition to accessing our district computer network, as the parent or legal guardian, I grant permission for the above named student to access the internet as well. This permission is granted for an indefinite period of time, unless otherwise requested. I understand that individuals and families may be held liable for violations of the Acceptable Use Rules and Procedures and District Policies. I understand that some materials on the internet may be objectionable, but I accept responsibility for guidance of Internet use – setting and conveying standards for my daughter or son to follow when selecting, sharing or exploring information and media.

Parent Name (Please Print) _____

Parent Signature _____ Date _____