Roma Independent School District
Acceptable Use Policy

I. General

Mission Statement

Effective performance of computer and telecommunications networks, whether local or global, relies upon end users adhering to established standards of proper conduct. The mission of this Acceptable Use Policy ("Policy" or "AUP") is to define the responsibilities of Roma Independent School District ("Roma ISD" or "District") employees and students (collectively, "Users") using computer, network and Internet resources (the "System"). In general, this requires efficient, ethical, and legal utilization of network resources. If a User violates any of these provisions, his or her access to the District's System will be denied and disciplinary action will be taken. The System, as with any other public resource, demands those entrusted with the privilege of its use be accountable. Use of the District's System during school and business hours must be (1) in support of education and/or research or (2) for school business, and (3) must support the mission of the District and (4) be in accordance with all School Board Policies and school regulations. Use of the District's System is a privilege, not a right.

Scope of AUP

This Policy address the acceptable conduct of both District students and employees. This Policy is meant to augment and not usurp other District policies regarding employee or student conduct.

This Policy will govern the use of all District System resources owned, leased, in the possession of, or otherwise provided by the District. Such resources include but are not limited to hardware, software, firmware, and Internet or network access. Additionally, all personal electronic devices will be governed by this Policy when such devices are connected to any portion of the District's System.

II. Acceptable Conduct and User Obligations

General

Use of the District's System is limited to educational purposes which include, but are not limited to, pursuing and promoting official District business, promoting educational excellence, resource sharing, facilitating innovative instruction and communication and preparing students to live and work in an increasingly technology-oriented society by providing them with electronic access to a wide range of information and the ability to communicate with others throughout the world. Further, the System will enable employees to improve skills and knowledge through the enhanced ability to exchange information with peers. The System will also assist the District in sharing information with the community, including parents, local, state and federal governmental departments, agencies, employees and businesses.

To ensure that all Users continue to benefit from the District's System, Users shall take affirmative steps to do the following:

1. Maintain passwords. Users are responsible for the use of their individual account and should take all precautions to prevent others from being able to access their account. Users should never disclose their passwords to others.

2. Report Security Issues. Users will immediately notify the District's Technology Coordinator if they have identified a possible security problem.

3. Respect Resource Limits. Users will use the District's System only for educational and professional activities during school and business hours. Any activity that does not fall within the Mission of this AUP and which degrades or taxes the System's resources is strictly prohibited. Examples of activities that degrade or tax System resources include, but are not limited to, sending mass unsolicited and unwanted email ("Spam"); attaching large files to email; and flooding servers.

4. Report Abusive Behavior. Students will promptly disclose to a teacher or other administrator or school employee any message they receive that is inappropriate, offensive or makes them feel uncomfortable.

III. Unacceptable Use

Users are prohibited from engaging in any behavior that is inconsistent with the Mission outlined in this Policy. Actions that constitute unacceptable uses of the District's System include, but are not limited to:

1. Hacking. Users will not attempt to gain unauthorized access to the District's system or to any other computer system through the District's system, or go beyond their authorized access. This includes attempting to log in through another account or accessing or attempting to access another person's files without authorization. These actions are prohibited, even if the User's intent is only to browse.

2. Spreading Malicious Code/Destroying Data. Users will not deliberately attempt to disrupt the District's system performance or destroy or alter other people's data by spreading computer viruses, worms, malicious code or by any other means.

3. Viewing Obscene Material. Users will not use the District's system to access, send, receive, view or download any obscene material or child pornography. Pursuant to the District's Internet Safety Policy, no student may access, send, receive, view or download any material that is harmful to minors.

4. Infringing Others' Copyrights. Users will not use the District's system to send, receive or download any copyrighted material for which they do not have a license to send, receive or download. Users will not receive or transmit any code, key, or other device that is used to circumvent a copyright protection scheme.

5. Engaging in Criminal Activity. Users will not engage in any illegal act, or in an act in furtherance of an illegal act. Examples of such illegal acts include, but are not limited to arranging for the sale/purchase of contraband, engaging in criminal gang activity, transferring stolen credit card information, gambling, or threatening the safety of another individual.

6. Annoying or Attacking Others. Users will not use the District's System to annoy, harass, threaten, or stalk any other person. Users will also not attack, flood, or engage in any other behavior that disrupts another's computer, system, or network.

7. Chatting. Unless otherwise authorized to do so by Faculty, Students may not use the District's System to engage in any form of real-time chatting. Examples of software used for real-time chatting include, but are not limited to, AOL Instant Messenger (AIM); Internet Relay Chat (IRC); ICQ; Yahoo Messenger; and Trillian.

8. Using Inappropriate Language. Students and employees will conduct themselves in a manner that is appropriate and proper as representatives of the school District. Users will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening or disrespectful language. Users will not engage in personal attacks, including prejudicial or discriminatory attacks. Restrictions against inappropriate language apply to public messages, private messages and material posted on the Internet.

9. Engaging in Tortious Conduct. Users may not engage in any conduct that causes harm to others. Examples of such conduct include engaging in fraud or knowingly or recklessly posting false or defamatory information about a person or organization.

10. Committing Plagiarism. Users will not use the District's System to take the ideas or writings of others and present them as if they were original to the User. Users will use proper methods of attribution.

IV. Privacy

1. Student Privacy. Unless authorized by Faculty (and then only if the attached "Release Form" has been properly executed) may students publish personally identifiable information about themselves or other students. Personally identifiable information includes a student's name, photograph, address, and telephone number.

2. Search and Seizure

Users have no right of privacy and should have no expectation of privacy in materials sent, received or stored in District owned computers or on the District's System. School officials reserve the right to review System use at any time to determine if such use meets the criteria set forth in School Board Policies and this AUP. Moreover, routine maintenance and monitoring of the system may lead to the discovery that the User has or is violating this Acceptable Use Policy, the Code of Student Conduct or other School Board Policies and regulations governing student or employee discipline or the law. Once a problem is discovered, an individual search will be conducted when there is a reasonable suspicion that the User has violated the law, the Code of Student Conduct or School Board Policies or regulations governing student discipline. The nature of the search/investigation will be reasonable and in keeping with the nature of the alleged misconduct.

Employees should be aware that their personal files may be subject to public inspection and copying under the Texas Open Records Act.

V. Parental Notification and Responsibility

The District will notify parents and legal guardians about the District's System and the School Board Policy and Acceptable Use Policy governing its use. Parents must sign this Acceptable Use Policy to allow their children to have access to the Internet. Parents who do not want their children to have access to the Internet may indicate so on this Acceptable Use Policy. Parents and legal guardians also have the right to revoke their permission and terminate a student's Internet access at any time.

The District will provide information to parents about the filtering software used by the District, describe the filtering levels in place at each level (elementary, middle and high school) and remind parents that the District cannot transmit the social values of the family to each child.

VI. Disclaimer and Limitation of Liability

Pursuant to the Children's Internet Protection Act, Roma ISD uses filtering software to screen Internet sites for offensive material. The Internet is a collection of thousands of worldwide networks and organizations that contain millions of pages of information. Users are cautioned that many of these pages contain offensive, sexually explicit, and inappropriate material, including, but not limited to the following categories: Adult Content; Nudity; Sex; Gambling; Violence; Weapons; Hacking; Racism/Hate; Tasteless; and Illegal/Questionable. In general it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. Additionally, having an e-mail address on the Internet may lead to receipt of unsolicited e-mail containing offensive content. Users accessing the Internet do so at their own risk. No filtering software is one hundred percent effective and it is possible that the software could fail. In the event that the filtering software is unsuccessful and children or staff gain access to inappropriate and/or harmful material, the District will not be liable. To minimize these risks, student use of the Roma ISD System is governed by this Policy.

THE DISTRICT MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, THAT THE FUNCTIONS OF THE SERVICES PROVIDED BY OR THROUGH THE DISTRICT'S SYSTEM WILL BE ERROR-FREE OR WITHOUT DEFECT. The District will not be responsible for any damage Users may suffer, 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 system. The District will not be responsible for financial obligations arising through the unauthorized use of the system.

VII. Due Process

The District will cooperate fully with local, state and federal officials in any investigation concerning or relating to any illegal activities conducted through the District's system.

In the event that there is an allegation that a student has violated this Acceptable Use Policy, the student will be provided with a written notice of the alleged violation and an opportunity to present an explanation before the District terminates his/her account privileges.

Disciplinary actions will be tailored to meet the specific concerns related to the violation and to assist the student in gaining the self-discipline necessary to behave appropriately on an electronic network. If the alleged infraction involves a violation of other provisions of the Code of Student Conduct or other School Board Policies and District Regulations governing student discipline, the violation will be handled in accordance with School Board Policies.

Employees violating this Acceptable Use Policy are subject to disciplinary action by the Superintendent or designee. Violations of this Acceptable Use Policy may subject the employee to disciplinary action up to and including dismissal, depending upon the nature of the violation. Violations of this Acceptable Use Policy will also be addressed by the Director of the Office of Technology who may terminate the system privileges of an employee by giving written notice of the alleged violation and the opportunity to respond.

I have read this Acceptable Use Policy and agree to abide by the terms of this Acceptable Use Policy.

Signature: ____

Date: ______________________________

PARENT OR GUARDIAN (If the User is under the age of 18, a parent or guardian must also read and sign this agreement.)

As the parent or guardian of *(Student's Name)* ______________________________________, I have read the Roma ISD Acceptable Use Policy. I understand that this access is designed for educational purposes and that Roma ISD has taken precautions to eliminate student access to certain material that may be offensive or harmful to minors. I also recognize, however, that it is impossible for Roma ISD to restrict access to all offensive material, and I will not hold the District responsible for material acquired on the network. Further, I accept full responsibility for supervision of my child when my child's use of the Internet is not in a school setting.

I hereby (check one)

____________ give permission for my child to access the Internet.

____________ do **NOT** give permission for my child to access the Internet.

Parent or Guardian (please print): ____

Signature:____ Date: ____________________

(Please return to your student's school.)

(Employees, please return to administrator in charge.)