Roma Independent School District
Acceptable Use Policy for Employees

I. General

Mission Statement

This policy is being provided so that employees are aware of the responsibilities they accept when they use District-owned computer hardware, operating system software, application software, stored text, data files, electronic mail, local databases, removable media, digitized information, communication technologies, and Internet access.

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 ("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 in support of education and/or research or for school business and must support the mission of the District and 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 addresses the acceptable conduct of District employees. This Policy is meant to augment and not usurp other District policies regarding employee conduct.

This Policy will govern the use of all District System resources owned, leased, in the possession of, or otherwise provided by the District. 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 business and educational purposes which include, but are not limited to, pursuing and promoting official District business, promoting educational excellence, research, resource sharing, facilitating innovative instruction, and communication. 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. Users must notify a campus or District administrator if they come across information or messages that are inappropriate, dangerous, threatening, or make them feel uncomfortable. Employees who identify or know about a security problem are expected to convey the details to their campus or district administrator without discussing it with others.

3. Respect Resource Limits. Users will use the District's System only for educational and professional activities during school and business hours. Users are responsible for conserving energy by turning off all electronic devices at the end of each business day. 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. Commercial/Political Activity. Users may not distribute advertisements, solicitations, commercial documents of any kind, or political materials via the District's System.

5. Personal Conduct and Accountability. Users are expected to be courteous and respectful in all communications. Users are personally responsible for their actions in accessing and utilizing the District's System. Employees are responsible for securing technology devices when not in use and for returning them in good working condition.

III. Unacceptable Use

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

1. Social Networking. Employees have a right to participate in social networking sites, blogs, forums, wikis, etc., or other Internet activities during their private time and for their private use; however, employees should not post anything (through written messages, images, videos, or otherwise that would violate student confidentiality rights, and/or District Board policies and procedures including but not limited to the Code of Ethics and Standard Practices for Texas Educators (as stated in Board policy DH (EXHIBIT), and/or that would negatively impact the perception of the employee's ability to be effective in their employment capacity. Postings that are considered inappropriate or otherwise are violations of District Board policies and procedures, including but not limited to the Acceptable Use Procedures, may be addressed by the District and could lead to disciplinary action up to and including termination.

2. Use of Pictures. Posting or transmitting pictures of students without obtaining prior permission from all individuals depicted or from parents of depicted students who are under eighteen years of age is prohibited.

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 employee may access, send, receive, view or download any material that is harmful to minors. A User who gains access to any inappropriate material is expected to discontinue the access immediately and to report the incident to a supervisor.

4. Infringing Others' Copyrights. All Users are expected to follow existing copyright laws. 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 Illegal Activity. Users will not engage in any illegal act, or in an act in furtherance of an illegal act. Users will not transmit any material that is in violation of any federal or state law. This includes, but is not limited to, student or other confidential information, copyrighted material, threatening or obscene material, and computer viruses. Other examples of such illegal acts include but are not limited to arranging for the sale/purchase of contraband, engaging in criminal activity, transferring stolen credit card information, gambling, contract violations or threatening the safety of another individual.

6. Annoying or Attacking Others. Users will not use the District's System to annoy, harass, threaten, bully, 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. Users will not use another person's account, password, or ID card or allowing another User access to your account, password, or ID.

7. Using Inappropriate Language. Employees will conduct themselves in a manner that is appropriate and proper as representatives of the 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.

8. 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.

9. 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.

10. Spreading Malicious Code/Destroying Data or Equipment. 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. Users are responsible to protect the System and all District equipment. Users should secure technology devices when not in use and return them in good working condition. Any malicious attempt to harm or destroy District equipment, data, or materials or to harm or destroy the data of another is prohibited.

11. Misuse of the System. Users may not access online videos, music, or streaming content that is unrelated to a District business purpose or educational curriculum. Users may not coach or otherwise assist or acquiesce in unauthorized activity on the System.

12. Harassment and Discrimination. Users may not use or access the System in a manner that violates the District's prohibitions against illegal harassment and discrimination. Users may not engage in sexual harassing conduct or use any language of a sexual or otherwise objectionable nature in public or private message.

13. Falsification of Records. Users may not access the System to falsify District records. Users may not access the System to alter District records in any manner that is not required by their jobs or for which authorization has not been specifically provided.

14. 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 prohibition 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.

15. Personal or Financial Gain. Users may not implement District resources for financial or commercial gain, advertising, or political activities.

16. Improper Use. Users may not use District System resources to access or explore online content that does not support the curriculum, is unrelated to legitimate school activities and/or is inappropriate for school assignments. Users may not cause congestion on the network or interfering with the work of others, e.g., chain letters, jokes, or pictures to lists or individuals. Users may not obtain copies of or modify files, data, or passwords belonging to other Users on the network without authorization.

IV. E-Mail

1. E-mail may be used for educational or administrative purposes only.

2. E-mail transmissions, stored data, transmitted data, or any other use of District owned technology by employees or any other user is subject to being monitored at any time by designated staff to ensure appropriate use.

3. All e-mail and all contents are property of the District.

V. Privacy

1. Student Privacy. In their use of District System resources Users may not do anything that would violate student confidentiality rights. Users may not publish personally identifiable information about 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 or other School Board Policies and regulations governing 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 or School Board Policies or regulations. 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 Public Information Act.

VI. Disclaimer and Limitation of Liability

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 authorized or 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.

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: _____

Printed Name: _____

Date: _____

(Employees, please return to administrator in charge.)