EDGEWOOD ISD ACCEPTABLE USE POLICY

A. Overview and Applicability

All District officers, Employees, Community Members, Students, Visitors and Volunteers of the Edgewood Independent School District shall abide by the policies and guidelines set forth in Board policy series CQ and in this document.

This Acceptable Use Policy ("Regulation") applies to District officers, Employees, Community Members, Students, Visitors and Volunteers (collectively "Users") who have access to and/or who attempt to access any of the following:

1. The District's electronic communication systems, including but not limited to the EDGENET System; and/or
2. The use of District-owned electronic equipment, software, operating systems, storage media, and/or network accounts that provide electronic mail, voice, fax and/or other forms of communications; and/or
3. Internet browsing and file, text and/or image transfers using District property or on District property through any means – for example: File Transfer Protocol (FTP), Hypertext Transfer Protocol (http) Graphical User Interfaces (GUI), and Transmission Control Protocol/Internet Protocol (TCP/IP);

all of which, individually and/or collectively, is referred to herein as "Network."

4. This Acceptable Use regulation is also applicable to any of the above using non-District property during District employment hours and/or while on District property.

Because of the need to protect the Network, the District does not guarantee the confidentiality of information created, exchanged and/or stored on the Network. For security, network maintenance, and/or other lawful purposes, authorized individuals may monitor the Network at any time and reserve the right to audit communication and data on a periodic basis to ensure compliance with this policy.

Edgewood ISD has the right to place reasonable restrictions on the use of equipment. Access to resources and materials by Students and Employees will be limited to login credentials as determined by the Technology Department. Students and Employees shall follow the rules set forth herein and in the District's policies, rules and regulations governing conduct, disciplinary code, and the law in their use of the Network.

All access and rights are privileges granted by the District, and users should expect no privacy rights. Access to the Network shall be primarily for instructional and/or administrative purposes. Limited personal use of the Network is permitted if such use:

1. Does not violate this regulation;
2. Is not illegal or a violation of a community or District standard;
3. Imposes no tangible cost on the District;
4. Does not unduly burden the District's Network resources;
5. Is not for a business purpose; and
6. Has no adverse effect on an Employee's job duties or performance or on a Student's academic performance.

B. System Security

Under no circumstances is any User authorized to engage in any activity involving the Network that is illegal under local, state, federal or international law. Should a User become aware of a violation of this Regulation, be informed of an alleged violation of this Regulation, or become aware of any possible security risk, the User shall immediately inform the Technology Department or the User's supervisor**.** In the case of a User Student, the Student shall notify the Student's teacher or counselor if the Student is unable to inform the Technology Department.

Except as otherwise permitted herein, Users shall not divulge their passwords to other persons except upon request by the Technology Department Administrator or an authorized technician in the Technology Department engaged in the technician's assigned duties or upon the request of the Superintendent or designee. Student-Users may reveal passwords to their teachers, Technology Department personnel and Administrators.

Users are responsible for the use of their individual access account and shall take all reasonable precautions to prevent others from being able to use their accounts. Students – Users are particularly cautioned not share their passwords with other Students. Those individuals in possession of Student passwords shall make every effort to protect the confidentiality of the passwords. Any User identified as a security risk or having a history of violating this Regulation may be denied access to the Network.

C. Network Activities and Software Use

Users must use all software in accordance with license agreements and the District's software standards. Only the Technology Department may install software and/or copy software for backup and archival purposes. Any User who determines that there may be a misuse/abuse of software licensing within the District shall immediately notify the Technology Administrator. All software used on the Network shall be purchased only through established District procedures.

The following activities are strictly prohibited, including but not limited to:

1. Installing and/or copying of any software on the Network, without the approval of the Technology Department.
2. Unauthorized use of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Edgewood ISD does not have an active license and/or has not been approved by the Technical Department for official District business.
3. Installing or reproducing unauthorized or unlicensed personal software or hardware on the Network.
4. Intentionally introducing malicious programs (e.g., viruses, worms, Trojan horses, e-mail bombs, etc).
5. Actively engaging in procuring or transmitting material that is in violation of sexual harassment or hostile workplace.
6. Circumventing User authentication or security.
7. Removing, modifying or circumventing Network technology equipment or software without written permission from the Technology Department.

D. E-mail and Communication Activities

Users shall have no expectation of privacy in anything they store, send or receive on the Network, including, without limitation, facsimiles, video mail messages, texting, voice-mail, whether a password is used or not.

The following activities are strictly prohibited, including but not limited to::

1. Creating messages that contain defamatory, obscene, offensive or harassing information or that discloses personal information without authorization.
2. Sending unsolicited non-work related e-mail messages, including creating and/or forwarding "chain letters" or "pyramid" schemes of any type or engaging in "spamming," which is defined as sending an annoying or unnecessary message to a large number of people.
3. Engaging in any form of harassment via e-mail, telephone or paging, whether through language, frequency, or size of messages.
4. Using Network e-mail for the creation or distribution of any disruptive or offensive messages.
5. Sending any unsolicited e-mail, either in bulk or individually, to any person who has indicated that they do not wish to receive it, before or after; except, however, work-related e-mail may not be blocked or unaccepted without prior written permission of a supervisor.
6. Forwarding a private e-mail message without permission of the sender; except, however, otherwise private e-mail messages shall be provided, when required, to authorized personnel undertaking an official investigation.
7. Except in accordance with the Public Information Act (Open Records Act) and District processing requirements for responding to requests for public information, providing District e-mail addresses to outside parties whose intent is to communicate with Employees, Students and their families without permission from the e-mail recipient and/or the Technology Department.
8. Sending sexually explicit material intended to cause sexual arousal through the Network, whether written or in attached documents, images, or web links.
9. Sending other material that is profane or obscene and/or otherwise violates the standard of conduct expected of District officers, Employees or Students.

E. Internet Access

In general, Users may have access to the Internet through the Network in accordance with their particular standing with the District. However, parents may specifically request that their children not be provided such access by notifying the District in writing.

No Student shall be given or have access to Network e-mail without a signed Parental Agreement. In recognition of the need to establish a safe and appropriate computing environment, the District shall use filtering technology to prohibit access, to the degree possible, to objectionable or unsuitable content that might otherwise be accessible via the Internet. The District shall filter the on-line activities of all Network computers with Internet access, as required by The Child Internet Protection Act (CIPA). Evading or disabling or attempting to evade or disable the District's content filtering device is prohibited. In making decisions to disable the District's filtering/blocking device for a specific site, the Technology Department designees shall consider whether the use will

serve a legitimate educational purpose or otherwise benefit the District.

When using District equipment, such as laptops, outside of the District, Employees shall continue to follow District policy as outlined by Board Policy series CQ and by this Regulation. Use of equipment on loan or lease to the District at any time or use of equipment for personal use on District property or during employment hours that accesses personal home networks, business networks and/or wireless (wifi) networks shall be bound by the constraints of this Regulation and must be used in a professional manner.

Edgewood ISD officers, Employees, Students, Community Members, Visitors and volunteer shall not engage in illegal, abusive, non-educational or irresponsible behavior. The following activities are strictly prohibited including, but not limited to:

1. Using the Network for non-instructional or non-administrative purpose other than for occasional, de minimis, personal use that meets the limited personal use standards outlined in this Regulation.
2. Using computer resources and Internet for private business activities, commercial purposes or for private financial gain.
3. Engaging in activities that result in excessive bandwidth use (e.g. streaming music, online-radio listening or non-educational video streaming).
4. Deliberately accessing, installing, downloading or creating sexually related materials except curriculum related and as otherwise authorized.
5. Engaging in non-educational games, chat rooms, and similar activities that are not authorized and are not for a primary District educational or administrative purpose.
6. Using the District Network to access material that is profane or obscene (pornography of any kind), that advocates illegal acts, or that advocates violence or discrimination towards other people (such as hate literature).
7. Using the District Network to solicit information with the intent of using such information to cause personal harm or bodily injury to others.
8. Posting information that could endanger an individual or cause personal damage.
9. Knowingly or recklessly posting prejudicial or discriminatory false or defamatory information about the school District, organization or person.
10. Posting online, or communicating to another person, information that is intended to ridicule or embarrass another person.
11. Making connections, whether directly or indirectly, that creates "backdoors" to established unauthorized access to the Network.
12. Using obscene, profane, lewd, vulgar, rude, inflammatory, hateful, threatening, or disrespectful language.
13. Plagiarizing works found on the Internet or other resources, or violating copyright law.
14. Using the Network for political lobbying or to advocate for or against a political candidate, office-holder, political party or measure, or to do harm to the District.

F. District Issued Devices

1. Applicable To Officers and Employees: Employees who have been issued District owned cell phones, laptops, iPads, netbooks or tablets must sign a District Technology Equipment Loan Agreement, follow any required additional guidelines attributed to them, and are responsible for their security and content at all times. As per the Loan Agreement, the Employee acknowledges that the District owns and shall retain title to the equipment and the Employee understands that he or she is responsible for loss, theft or damage to the equipment on or off the district's property.

The Employee shall report loss, theft or damage of the Equipment to the campus administrator and the Inventory Department within the next working day; and shall immediately report any theft or mysterious disappearance to the appropriate law enforcement authority and provide the District with a copy of the incident report as soon as reasonably practicable. Failure to follow this protocol shall result in adverse employment action against the Employee. The Employee agrees to submit to the District, any recovered insurance proceeds from the loss, theft or damage of the Equipment within 5 days of receipt to the District.

A District-owned device shall not be used off of school property or outside a school-sponsored event unless the Employee has agreed to and has executed an agreement with the District for financial responsibility of the device on the District's form contract entitled "Agreement for Assumption of Financial Responsibility for Use of Electronic Equipment Off School Property or Outside of a School-Sponsored Event."

Devices shall be password-protected and secured with a locking system. Employees shall make every reasonable effort to secure the devices while they are not in use. All repairs and/or warranty-related service shall be handled through the Technology Department. Employees are prohibited from contacting the manufacturer directly for repairs or service.

2. Applicable to Students: Each Student, or the Student's parent or guardian, is responsible for each electronic textbook and all technological equipment not returned in an acceptable condition by the Student. A Student who fails to return in an acceptable condition all electronic textbooks and technological equipment forfeits the right to free electronic textbooks and technological equipment until each electronic textbook and all technological equipment previously issued but not returned in an acceptable condition is paid for by the Student, parent or guardian; except, however, the Board of Trustees may waive or reduce the payment requirement if the Student is from a low-income family. The District shall not, however, disallow a Student who does not return or pay for such equipment to use electronic textbooks and technological equipment at school during each school day, but the District may withhold the Student's records.

G. Personal Hand Held Devices

1. Cell Phones, etc. Using personal handheld communication devices (cell phones, etc.) that use any medium to synchronize, transmit, share or access files on remote computers or District servers is permitted with some limitations. These devices should not impede with the Network traffic nor interrupt services to Students. Users of personal devices must refrain from their use for non-instructional purposes. Personal handheld devices shall not be used to access inappropriate material while in District or at District

events and Students are prohibited from using personal devices unless in response to an emergency situation or teacher approved instructional use.

2. Portable Data Drives (e.g. thumb drives, flash drives, jump drives, etc.) are permitted; however, Users are prohibited from installing or downloading offensive material, malicious programs and/or any data that is in violation of this Regulation. Visitors to the district are not allowed to save any data from the Network without prior approval from the Technology Department.

H. Non-District Users

Non-District Users shall first obtain and use a "Guest" password that limits their access to the Network. Once access is gained, the Authorized Use Policy applies to all.

I. Responsibilities to Students

Employees shall adhere to online safety guidelines when working with Students in accordance with the Family Educational Rights and Privacy Act (FERPA). Student photographs and/or work that appear(s) on any District documents and/or web pages shall not identify Students with their full name. Any Student or Student's parent, guardian or other person in lawful control of the Student who does not want the Student's image or work to be displayed on the Network shall notify the District by declining permission on the Student User Agreement Form in the Student handbook during the first week of attendance.
District Students shall have the written approval of a parent, guardian or other person in lawful control of the Student in order to access the Network. This signed Student Access Form must be on file with the District's designee for each campus as assigned by the Principal. Student privileges and access will be granted only for one academic year and will terminate once a Student withdraws from the District. The Student Access Form shall indicate that the person signing the permission form has read and understands the form and any supplemental information that may be provided with the permission form and agrees to adhere to the guidelines established in this Regulation. Student Access Forms shall include a provision that the Student and his/her custodial parents or Guardians have/has agreed to hold the District harmless from Student violations of guidelines and regulations of this Regulation.

Employees and Volunteers who utilize the Network for instructional purposes also have a responsibility to supervise Student use to help ensure that Students are using the Network appropriately and responsibly.

Employees and Volunteers are expected to be familiar with this Regulation and all other applicable rules concerning Student Network use and to enforce them. In the course of their duties, should any Employee or volunteer become aware of Student violations, they shall be expected to stop the activity and inform the building Principal, Campus Technology Teacher, and the Technology Administrator's designees.

J. User Acknowledgement Required

Annually, every Network User shall sign an Acceptable Use Policy Acknowledgement Form stating that he or she has read this Regulation, understands it, and agrees to adhere to the rules set forth herein. The Acknowledgement Form shall be retained in the Human

Resources Department as part of the Employee-User's file for the length of the employee of the user. In the case of the non-Student, non-Employee Users, the forms shall be maintained with the Technology Department. In the case of the Student-Users, the forms shall be maintained with the Student's Principal.

This Acknowledgement Form for all users needs to be completed out at the start of each academic year.

K. Due Process

The District shall cooperate fully with local, state, or federal officials in any investigation concerning or relating to any illegal activities conducted by Network Users. In the event there is an allegation that a Student has violated the District's acceptable use of the Network, the Student shall be provided with a written notice of the alleged violation and shall be provided with notice and an opportunity to be heard in the manner set forth in the Student Hearing Process Policy. Disciplinary actions may be taken.

In the event there is an allegation that an Employee has violated the District's acceptable use of the Network, the Employee shall be provided with notice and an opportunity to respond in writing. Employees violating the District's acceptable use of the Network may have their privileges suspended or revoked and shall be subject to other disciplinary actions in accord with the law and District School Board Policy.

L. Administration

The District Technology Administrator has the responsibility and authority for the development, publication, implementation and ongoing administration and enforcement of the processes and techniques required to protect the Network from unauthorized access, loss or misuse. Department Directors and/or Coordinators have the responsibility to establish a plan to ensure adequate supervision of Employees. School Principals have the responsibility to establish a plan to ensure adequate supervision of Students.